SnapServer®

Administrator Guide

GuardianOS v6.0

For GuardianOS-powered SnapServers and Expansion Arrays

10400272-001

www.overlandstorage.com

COPYRIGHT

TRADEMARKS

REVISIONS

Overland Storage, Inc. provides this publication “as is” without warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability or fitness for a particular purpose. Overland Storage and its subsidiaries reserve the right to revise this publication and to make changes in the content hereof without the obligation of Overland Storage to notify any person of such revision or changes.

END USER LICENSE AGREEMENT (EULA)

FOR USE OF OVERLAND STORAGE STORAGE SOLUTIONS AND RELATED INSTALLATION UTILITIES

SNAP IP, ASSIST, AND SNAPSERVER MANAGER ("INSTALLATION UTILITIES"); THE SYSTEM SOFTWARE EMBEDDED IN THE SNAPSERVER STORAGE SOLUTION ("EMBEDDED SOFTWARE"); SOFTWARE MARKETED BY OVERLAND STORAGE OR THAT IS EMBEDDED IN OR OTHERWISE CONSTITUTES A PART OF OVERLAND STORAGE COMPUTER HARDWARE PRODUCT(S) (SOMETIMES REFERRED TO COLLECTIVELY HEREIN, TOGETHER WITH THE INSTALLATION UTILITIES AND THE EMBEDDED SOFTWARE, AS THE "LICENSED SOFTWARE"), EXCEPT WHERE EXPRESSLY PROVIDED OTHERWISE, ARE PROPRIETARY COMPUTER SOFTWARE BELONGING TO OVERLAND STORAGE, INC. OR ITS LICENSORS. UNITED STATES COPYRIGHT AND OTHER FEDERAL AND STATE LAWS AND INTERNATIONAL LAWS AND TREATIES PROTECT THE INSTALLATION UTILITIES AND EMBEDDED SOFTWARE.

USE OF THE SNAPSERVER STORAGE SOLUTION ("SERVER") OR THE INSTALLATION UTILITIES IMPLIES YOUR AGREEMENT TO THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT. BY USING THE INSTALLATION UTILITIES OR THE SERVER, YOU ARE ENTERING INTO A BINDING CONTRACT WITH OVERLAND STORAGE, INC. IF YOU DO NOT AGREE TO BE BOUND BY THESE TERMS AND CONDITIONS, YOU MAY NOT USE THE INSTALLATION UTILITIES, THE EMBEDDED SOFTWARE, OR THE SERVER AND SHOULD PROMPTLY RETURN THIS ENTIRE PACKAGE, INCLUDING THE INSTALLATION UTILITIES AND SERVER, TO THE PLACE WHERE YOU PURCHASED IT FOR A FULL REFUND.

1 Ownership and Copyright. The Installation Utilities and Embedded Software are licensed, not sold to you, for use only as permitted by the terms and conditions of this Agreement. Overland Storage reserves any rights not expressly granted to you. The Licensed Software is composed of multiple, separately written and copyrighted modular software programs. Various Licensed Software programs (the "Public Software") are copyrighted and made available under the GNU General Public License or other licenses that permit copying, modification and redistribution of source code (which licenses are referred to as "Public Licenses").

The Public Software is licensed pursuant to (i) the terms of the applicable Public License located in the related software source code file(s), and/or in its on-line documentation; and (ii) to the extent allowable under the applicable Public License. The GPL and source code are available at oss.snapserver.com. To receive a copy of the GNU General Public License, write to the Free Software Foundation, Inc., 59 Temple Place - Suite 330, Boston, MA 02111-1307, USA.

Various Public Software programs are copyrighted by the Regents of the University of California and are derived from material licensed to the University of California by its contributors, to which the following disclaimer applies:

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

All other Licensed Software programs (the "Restricted Software") are copyrighted by Overland Storage or its licensors and are licensed pursuant to all of the terms of this Agreement.

Copying of the Licensed Software, unless specifically authorized in writing by Overland Storage, is prohibited by law. You may not use, copy, modify, sell, lease, sublease, or otherwise transfer the Installation Utilities or Embedded Software, or any copy or modification, in whole or in part, except as expressly provided in this Agreement.

PROVISIONS APPLICABLE TO RESTRICTED SOFTWARE ONLY (ARTICLES 2 - 7):

2 License. In consideration of the premises of this License Agreement, your payment of any applicable license fee for Restricted Software, and/or your purchase of a SnapServer that the Licensed Software accompanies, for the term of intellectual property protection inhering in the Licensed Software, Overland Storage hereby grants to you a limited, personal, and non-exclusive license to install and execute ("Use") the Restricted Software solely under the terms and conditions of this Agreement and only on the Server in connection with which Overland Storage originally provided such Restricted Software. You are given a non-exclusive license to use the Installation Utilities and Embedded Software in conjunction with a Server, make one copy of the Installation Utilities for archival and backup purposes only, and/or transfer your Server and copies of the Installation Utilities and the accompanying documentation to a third party provided that you provide Overland Storage written notice of the transfer within 30 days after the transfer date and you do not retain any copy of the transferred software. Any such transferee's rights and obligations with respect to the transferred software and documentation are as set forth in this Agreement.

3 Reproduction of Proprietary Notices. You may not sublicense, distribute, rent, lease, lend, or otherwise convey the Restricted Software or any portion thereof to anyone, and under no circumstance may you use or allow the use of the Restricted Software in any manner other than as expressly set forth herein. Copies of the Installation Utilities must be labeled with the Overland Storage copyright notice and other proprietary legends found on the original media.

4 Protection of Trade Secrets. The Licensed Software contains trade secrets, and in order to protect them, you agree that you will not reverse assemble, decompile or disassemble, or otherwise reverse engineer any portion of the Restricted Software, or permit others to do so, except as permitted by applicable law, but then only to the extent that Overland Storage (and/or its licensors) is not legally entitled to exclude or limit such rights by contract. Except with respect to online documentation copied for backup or archival purposes, you may not copy any documentation pertaining to the Licensed Software. You agree that your use and possession of the Licensed Software is permitted only in accordance with the terms and conditions of this Agreement.

5 Ownership of Restricted Software. You agree and acknowledge that, (i) Overland Storage transfers no ownership interest in the Restricted Software, in the intellectual property in any Restricted Software or in any Restricted Software copy, to you under this Agreement or otherwise, (ii) Overland Storage and its licensors reserve all rights not expressly granted to you hereunder, and (iii) the Restricted Software is protected by United States Copyright Law and international treaties relating to protection of copyright, and other intellectual property protection laws of the U.S. and other countries.

6 Termination. If you fail to fulfill any of your material obligations under this Agreement, Overland Storage and/or its licensors may pursue all available legal remedies to enforce this Agreement, and Overland Storage may, at any time after your default of this Agreement, terminate this Agreement and all licenses and rights granted to you hereunder. You agree that any Overland Storage suppliers referenced in the Restricted Software are third-party beneficiaries of this Agreement, and may enforce this Agreement as it relates to their intellectual property. You further agree that, if Overland Storage terminates this Agreement for your default, you will, within thirty (30) days after any such termination, deliver to Overland Storage or render unusable all Restricted Software originally provided to you hereunder and any copies thereof embodied in any medium.

7 Government End Users. The Installation Utilities, Embedded Software, and accompanying documentation are deemed to be "commercial computer software" and "commercial computer software documentation," respectively, pursuant to DFAR Section 227.7202, Commercial Computer Software-Restricted Rights at 48 CFR 52.227-19, and FAR Section 12.212, and successor provisions thereof, as applicable. Any use modification, reproduction release, performance, display, or disclosure of the Installation Utilities or Embedded Software and accompanying documentation by the U.S. Government shall be governed solely by the terms of this Agreement and shall be prohibited except as expressly permitted by the terms of this Agreement.

PROVISIONS APPLICABLE TO RESTRICTED SOFTWARE AND, SUBJECT TO SECTION 1, TO PUBLIC SOFTWARE (ARTICLES 8 - 15):

8 Export Laws. Notwithstanding any provision of any Public License to the contrary, Overland Storage shall have no duty to deliver or otherwise furnish source code of any Public Software if it cannot establish to its reasonable satisfaction that such delivery or furnishing will not violate applicable US laws and regulations. You hereby assure that you will not export or re-export any Licensed Software except in full compliance with all applicable laws, regulations, executive orders, and the like pertaining to export and/or re-export, including without limitation USA versions of the same. No Licensed Software may be exported or re-exported into (or to a national or resident of) any country to which the U.S. embargoes goods, or to anyone on the U.S. Treasury Department's list of Specially Designated Nationals or the U.S. Commerce Department's Table of Denial Orders. You agree to ascertain necessary licensing procedures and obtain required licenses before exporting or re-exporting either. You also agree to indemnify Overland Storage and assume all financial responsibility for any losses it may suffer if you do not comply with this paragraph.

9 Disclaimer of Warranties. THE INSTALLATION UTILITIES AND EMBEDDED SOFTWARE ARE LICENSED "AS IS" WITHOUT WARRANTY OF ANY KIND. OVERLAND STORAGE HEREBY DISCLAIMS ALL WARRANTIES, EXPRESS AND IMPLIED, RELATING TO THE INSTALLATION UTILITIES AND THE EMBEDDED SOFTWARE INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT.

10 Limitation of Liability. IN NO EVENT WILL OVERLAND STORAGE OR ITS LICENSORS' LIABILITY UNDER THIS AGREEMENT EXCEED THE PRICE THAT YOU PAID FOR THE INSTALLATION UTILITIES AND EMBEDDED SOFTWARE. FURTHERMORE, IN NO EVENT WILL OVERLAND STORAGE OR ITS LICENSORS BE LIABLE FOR ANY LOST PROFITS, LOST DATA, COST OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, INDIRECT, OR PUNITIVE DAMAGES ARISING OUT OF OR UNDER THIS AGREEMENT OR THE APPLICABLE PUBLIC LICENSE. The limitation of liability set forth in this paragraph will apply whether or not Overland Storage or its licensor was advised of the possibility of the loss, liability, or damages and notwithstanding any failure of essential purpose of any limited remedy. Since some states do not allow exclusions or limitations of liability for consequential or incidental damages, this provision may not apply to you.

11 Waiver. No delay or failure of Overland Storage to exercise any right under this Agreement, nor any partial exercise thereof, shall be deemed to constitute a waiver of any rights granted hereunder or at law.

12 Unlawful Provision(s). If any provision of the Agreement is held to be unenforceable for any reason, all other provisions of this Agreement shall nevertheless be deemed valid and enforceable to the fullest extent possible.

13 Applicable Law. Except with respect to any Public Software program for which the applicable Public License contains provisions expressly stating the applicable governing law (with respect to which the law so specified shall govern all aspects of such agreement, including the provisions incorporated into such Public License hereunder), the terms of this Agreement (including, to the extent allowable under the Public License, all software governed by a Public License which does not specify a governing law) will be governed by the laws of the State of California, without reference to its choice of law rules, and the United States, including U.S. Copyright laws.

14 Entire Agreement. This Agreement and all applicable Public Licenses supersede all proposals, negotiations, conversations, discussions, all other agreements, oral or written, and all past course of dealing between you and Overland Storage relating to the Licensed Software or the terms of its license to you, and may only be modified in writing signed by you and Overland Storage.

15 Contractor/Manufacturer. Overland Storage, Inc. 4820 Overland Avenue, San Diego, CA 92123.

COMPUTER ASSOCIATES INTERNATIONAL, INC. ("CA")

ETRUST ANTIVIRUS

END USER LIMITED LICENSE AGREEMENT (THE "AGREEMENT")

CAREFULLY READ THE FOLLOWING TERMS AND CONDITIONS REGARDING YOUR USE OF ETRUST ANTIVIRUS, INCLUDING ITS CODE AND DOCUMENTATION (THE "PROGRAM") BEFORE USING THE PROGRAM.

1 CA PROVIDES YOU WITH ONE COPY OF THE PROGRAM AND LICENSES THE PROGRAM TO YOU PURSUANT TO THE TERMS OF THIS AGREEMENT.

a. The Program is provided solely for your nonexclusive, limited use for a single user and a single CPU for your internal data processing purposes. You may not transfer the Program to another CPU or site or upgrade the CPU without the payment of CA's applicable fees. You may NOT exceed this usage limitation.

b. If the Program is a beta program and not generally available to date, CA does not guarantee that the generally available release will be identical to the beta program or that the generally available release will not require reinstallation. You agree that if otherwise required by CA, you shall provide CA with specific information concerning your experiences with the operation of the Program.

c. If the Program is an evaluation version, you agree to use the Program solely for evaluation purposes, in accordance with usage restrictions set forth in Section 1(a), for the thirty-day evaluation period. At the end of the evaluation period, you agree to return to CA all copies or partial copies of the Program or certify to CA that all copies or partial copies of the Program have been destroyed from your computer libraries and/or storage devices. You agree and acknowledge that the evaluation version of the Program will not operate after the expiration of the evaluation period.

d. You may copy the Program solely for backup or archival purposes. The Program is a trade secret of CA and confidential information of CA and its licensors. You agree to keep the Program strictly confidential and not to disclose the Program nor allow anyone to have access to the Program other than your authorized employees. Title to the Program and all changes, modifications and derivative works thereto shall remain with CA and its licensors. The Program is protected by copyright, patent, trademark and other laws and international treaties.

2 Without the prior written consent of CA, you may not:

a. Transfer, assign, use, copy, distribute or modify the Program, in whole or in part, except as expressly permitted in this Agreement;

b. Decompile, reverse assemble or otherwise reverse engineer the Program, except as expressly permitted under applicable law;

c. Remove or alter any of the copyright notices or other proprietary markings on any copies of the Program; or

d. Perform, publish or release benchmarks or other comparisons of the Program without CA's prior written consent.

3 CA may immediately terminate this Agreement in the event of any failure to comply with any of the above terms. Such termination shall be in addition to and not in lieu of any criminal, civil or other remedies available to CA.

4 CA DOES NOT WARRANT THAT THE PROGRAM WILL MEET YOUR REQUIREMENTS OR THAT THE OPERATION OF THE PROGRAM WILL BE UNINTERRUPTED, ERROR FREE OR WILL APPEAR AS DESCRIBED IN THE DOCUMENTATION.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW: (A) THE PROGRAM IS PROVIDED "AS IS," WITHOUT WARRANTY OF ANY KIND; (B) CA AND ITS LICENSORS DISCLAIM ALL WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE; AND (C) IN NO EVENT WILL CA OR ITS LICENSORS BE LIABLE FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, INCLUDING TIME, MONEY, GOODWILL AND ANY INCIDENTAL, INDIRECT OR CONSEQUENTIAL DAMAGES, ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM EVEN IF CA HAD BEEN ADVISED OF THE POSSIBILITY OF SUCH LOSS OR DAMAGES.

5 You acknowledge that the Program is provided with "Restricted Rights" as set forth in 48 C.F.R. Sec. 12.212, 48 C.F.R. Sec. 52.227-19(c)(1) and (2) or DFARS Sec. 252.227.7013(c)(1)(ii) or such applicable successor provisions. CA is the manufacturer of the Program. This Agreement shall be construed according to and governed by the laws of the State of New York. You are required to observe the relevant US Export Administration Regulations and other applicable regulations. Outside the United States, no product support services, if available, will be offered by CA without a proof of purchase or license from an authorized source.

Any questions concerning this Agreement should be referred to Computer Associates International, Inc., One Computer Associates Plaza, Islandia, NY 11749.

BY USING THIS PRODUCT, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS AGREEMENT AND THAT YOU ACCEPT ITS TERMS AND CONDITIONS. YOU ALSO AGREE THAT THIS AGREEMENT CONSTITUTES THE COMPLETE AGREEMENT BETWEEN US REGARDING THIS SUBJECT MATTER AND THAT IT SUPERSEDES ANY INFORMATION YOU HAVE RECEIVED RELATING TO THE SUBJECT MATTER OF THIS AGREEMENT, EXCEPT IF THIS AGREEMENT IS SUPERSEDED IN ITS ENTIRETY BY ANOTHER WRITTEN AGREEMENT, EXECUTED BY BOTH YOU AND CA, GRANTING YOU A LICENSE TO USE THE PROGRAM. THIS AGREEMENT MAY ONLY BE AMENDED BY A WRITTEN AGREEMENT SIGNED BY AUTHORIZED REPRESENTATIVES OF BOTH PARTIES.

Contents

Preface

Audience and Purpose

This guide is intended for system and network administrators charged with installing and maintaining SnapServers on their network. We assume the administrator is familiar with the basic concepts and tasks of multiplatform network administration.

This guide provides information on the installation, configuration, security, and maintenance of SnapServers. It also provides information on installing and using the following utilities and software components:

- The Administration Tool
- SnapServer Manager (SSM)
- VSS/VDS Hardware Provider
- Computer Associates eTrust Antivirus (CA *e*Trust Antivirus)
- Third-party backup agents

Some of the information presented in this manual (particularly the Storage Configuration and Expansion sections) applies only to SnapServers with four (4) or more drives. Users of the SnapServer 110 and SnapServer 210 are encouraged to consult the *User's Guide for SnapServer 110 and 210* as their primary reference and to refer to this Administrator's Guide for advanced guidelines.

Service and Technical Support

For an immediate response to a service inquiry, use our Expert Knowledge Base System at http://www.snapserver.com/kb. If you are unable to resolve your issue through the Knowledge Base, you can forward the question to our Technical Support department who will then e-mail you with a response. To obtain additional service or technical support for your SnapServer, call 1.888.343.SNAP.

Notes and Cautions

Conventions used to call out useful or important information are described below:

Note A note presents time-saving shortcuts related to the main topic.

Note A caution alerts you to potential hardware or software issues or hazards in the configuration or operation of SnapServers. Consider cautions carefully before proceeding with any operation.

Typographical Conventions

Convention	Usage
Italic	• Emphasis • The introduction of new terms • File names • Settings you select or enter in the Administration Tool
Arial Bold	Navigational paths, command buttons, and navigational links.
Arial	• Text you type directly into a text field, a command line, or a Web page • Buttons on a keyboard
Courier Italic	A variable for which you must substitute a value
`Courier Bold`	Commands you enter in a command-line interface
`Right-Click`	This document uses the Windows convention in describing keyboard access to context-sensitive menus. For example, “To rename a group, right-click a group and then select Rename.” Macintosh users should substitute control-click to achieve the same result.

Finding More Information

Product documentation related to GuardianOS SnapServers and expansion arrays are listed below. The current versions of all these documents are always available from http://www.snapserver.com/support.

Source and Location	Content
Quick Start Guide Product Packaging and Web	Details package contents, identifies server hardware components, and provides complete instructions for installing the server to a rack and connecting the server to the network. Also contains the EULA and warranty.
SnapServer Administrator Guide User CD and Web **SnapServer Online Help** Administration Tool	Provides an overview of the configuration, maintenance, and troubleshooting of SnapServers, the administration of the CA *e*Trust Antivirus software, the installation of third-party backup agents, and detailed instructions on using the Administration Tool.
Hardware Configuration and Options Guide User CD and Web	Lists hardware specifications for SnapServers and Snap Disk expansion arrays.
User Guide for SnapServer 110 and 210	Provides an overview of the configuration and maintenance of the SnapServer 110 and 210.
Release Notes.html User CD	Contains late-breaking information, corrections, and known issues concerning SnapServers.
Upgrade.html User CD	Provides instructions for upgrading the GuardianOS software.
SnapServer tools (SnapServerToolsInstall) User CD	Provides instructions for installing the SnapServer Manager administrative utility and, on supported Windows platforms, the VSS/VDS Hardware Provider.
Snap EDR Documentation Web	Software and complete Snap EDR documentation set are available at the SnapServer web site: http://www.snapserver.com/support.
NetVault Documentation Product Packaging and User CD	Provides a Client Installation Guide and the NetVault CD. The NetVault CD includes the complete NetVault documentation set.
Customer Spares Documentation Service CD and Web	Provides detailed instructions for the replacement of disk drives, adapter cards, power assemblies, slide rails, and other hardware components.

Administrative Overview

SnapServers are designed as flexible, low-maintenance network file servers optimized for performance and efficiency. SnapServers run the GuardianOS, built to maximize file I/O throughput across multinetwork protocols. To this end, all unnecessary system control and processing functions that are associated with a general-purpose server have been removed. This guide applies to the following SnapServers and expansion arrays:

Snap Unit	Description
SnapServer 110	The SnapServer 110 is a desktop file server with one disk drive and four USB ports.
SnapServer 210	The SnapServer 210 is a desktop file server with two disk drives and four USB ports.
SnapServer 410	The SnapServer 410 is a 1U departmental file server with four hot-swappable SATA disk drives and four USB ports.
SnapServer 520	The SnapServer 520 is a 1U departmental file server with four hot-swappable SATA disk drives. The SnapServer 520 supports multiple Snap Expansion S50 expansion arrays.
SnapServer 620	The SnapServer 620 is a 1U departmental file server with four hot-swappable SATA disk drives and a dual-core CPU. The SnapServer 60 supports multiple Snap Expansion S50 expansion arrays.
SnapServer 650	The SnapServer 650 is a 1U enterprise file server with four hot-swappable SAS disk drives, two dual-core CPUs, and dual power supplies. The SnapServer 650 supports multiple Snap Expansion S50 expansion arrays.
SnapServer NAS N2000	The SnapServer NAS N2000 is a 2U enterprise file server with 4 to 12 hot-swappable SATA II or SAS disk drives, a dual-core CPU, and dual power supplies. The SnapServer N2000 supports multiple SnapServer EXP E2000 expansion arrays.

Snap Unit	Description
SnapServer EXP E2000	The SnapServer EXP E2000 is a 2U expansion array with up to 4 to 12 hot-swappable SATA II or SAS disk drives. It can be used to expand the capacity of the SnapServer NAS N2000.
Snap Expansion S50	The Snap Expansion S50 is a 2U expansion array with up to up to 12 hot-swappable SAS or SATA disk drives. It can be used to expand the capacity of the SnapServers 520, 550, 620, 650, 4500, and 18000.

GuardianOS Specifications

These specifications apply to all SnapServers and expansion arrays running the most recent version of GuardianOS.

Feature	Specification
Network Transport Protocols	TCP/IP UDP/IP AppleTalk
Network Block Protocols	iSCSI
Network File Protocols	Microsoft Networking (CIFS/SMB) UNIX Network File System (NFS) 2.0/3.0/4.0 AppleTalk Filing Protocol (AFP) v2.0/v3.1 Hypertext Transfer Protocol (HTTP/HTTPS) File Transport Protocol (FTP/FTPS)
Network Client Types	Microsoft Windows 95/98/ME/NT 4/2000/XP/2003/2008/Vista/7 Macintosh Systems OS 9.x, 10.x Sun Solaris 9/10 HP-UX 11 AIX 5.3 Red Hat Linux 9.0 Red Hat Enterprise Linux (RHEL) 3.x, 4.x Red Hat Fedora Core 4.x + SuSE Pro 9.x, 10.x SuSE Linux Enterprise Server (SLES) 8.x, 9.x, 10.x

Feature	Specification
Server Emulation	Windows 2000/2003/2008/NT 4 AppleShare 6.0 Network File System (NFS) 2/3/4 Windows Print Server IPP Print Server
Network Security	CA *e*Trust Antivirus software Microsoft Active Directory Service (ADS) (member server) Windows NT Domain (member server) UNIX Network Information Service (NIS) File and Folder Access Control List (ACL) Security for Users and Groups Secure Sockets Layer (SSL v2/3) 128-bit Encryption Target Challenge Handshake Authentication Protocol (CHAP) for iSCSI SMTP Authentication and support for email encryption (STARTTLS and TLS/SSL encryption protocols)
Data Protection	Snapshots for immediate or scheduled point-in-time images of the file system Local Backup with BakBone Netvault Workgroup Edition Network Backup with VERITAS NetBackup/Backup Exec, CA BrightStor ARCserve, EMC Legato NetWorker, or BakBone NetVault APC-brand Uninterruptable Power Supply (UPS) with Network Management Cards, a USB interface, or a serial interface (with USB to serial adapter) are supported for graceful system shutdown

Feature	Specification
System Management	Browser-based Administration Tool for remote system administration SnapCLI for volume system deployment SnapServer Manager utility (platform independent) SNMP (MIB II and Host Resource MIB) User disk quotas for Windows, UNIX/Linux, Mac, FTP/FTPS Group disk quotas for UNIX/Linux Environmental monitoring Email event notification and SNMP trap notification Data migration

Feature	Specification
RAID Options	**RAID 0 (drive striping):** Large virtual drive with data striped across all drives of the array to provide maximum performance with no loss in usable capacity. Does not provide data protection. **RAID 1 (drive mirroring):** One or more drives duplicate one drive for maximum data protection. **Note** Available only on systems with two (2) or more drives. **RAID 5 (drive striping with parity):** For each array, the size of one drive is reserved for parity. Provides good performance and space utilization with one-drive fault tolerance. **Note** Available only on systems with four (4) or more drives. **RAID 6 (drive striping with two parity drives):** Like a RAID 5 except that two drives are used for parity rather than one. Provides moderate performance and reasonable space utilization with two-drive fault tolerance. **Note** Available only on systems with four (4) or more drives. **RAID 10 (striped mirroring):** A combination of RAID 0 and RAID 1. Provides high performance and fault tolerance. **Note** Available only on systems with four (4) or more drives. **Global or local hot spare support** **Instant Capacity Expansion (ICE):** Logically groups RAIDs for dynamic online scalability.
DHCP Support	Supports Dynamic Host Configuration Protocol (DHCP) for automatic assignment of IP addresses

What's New in GuardianOS

The following tables list the new and changed features since GuardianOS v3.2.

What's New in GuardianOS v6.0

GuardianOS 6.0 has the following new features and functionality:

Feature	New Functionality
Support for Multiple Ethernet Ports	With the installation of an Ethernet card, the SnapServer NAS N2000 supports up to 6 ethernet ports.
Write Cache Option	Write cache can now be disabled on a volume, allowing data to be written directly to the disk. **Note** For this feature to be available, all drives on the volume must support disabling of write cache. SnapServers and expansions with IDE drives (SnapServer 4200, 4400, 4500, SD10), SnapServer 18000, and SD30 do not support disabling write cache.
Email Authentication and Encryption Capability	SMTP Authentication and Secure Connection have been added to the SnapServer email capabilities.
Wake-on-LAN	SnapServer NAS N2000 supports Wake-on-LAN on Ethernet 1 and Ethernet 2.

What's New in GuardianOS v5.2

GuardianOS 5.2 has the following new features and functionality:

Feature	New Functionality
VSS/VDS Support for iSCSI	VSS (Volume Shadow Copy Service) and VDS (Virtual Disk Service) Hardware Providers have been added for SnapServer iSCSI targets. VSS provides a mechanism by which application-consistent snapshots of iSCSI targets may be taken without performing full application (or system) shutdown, for backup or other purposes. The VDS feature allows a Windows administrator to natively manage iSCSI storage, using any VDS compliant management console application.
Password Policies	The administrator can now set password policies for local users to establish requirements, expiration dates, and automatic lockout.

Feature	New Functionality
User Interface Enhancements	The User Interface now comes in three color schemes: green slate, azure sea, and golden desert.
Windows 2008 Domain Support	Windows domains hosted by Windows 2008 servers are now supported.
Support for 128-bit SMB Encryption	GuardianOS now supports 128-bit encrypted communcation with SMB clients and servers.
File Security Viewing	When logged in as an administrator, files and folders in Web View now display a security icon (key) that, when clicked, shows security information about the file/folder.
Root Filesystem Check	The WebUI now provides the ability to check the root filesystem for errors and repair if found.

What's New in GuardianOS v5.1

GuardianOS 5.1 has the following new features and functionality:

Feature	New Functionality
Web root capability	The SnapServer can now serve a default web root share and web page when users connect to the server via a web browser.
Automatic software update notification	The WebUI displays an alert whenever software updates for GuardianOS or Snap EDR are available. In addition, SSM displays an alert when GuardianOS updates are available for any discovered servers, and lists the available updates per server.
NFSv4 RPCSEC GSS (Kerberos) support	Unix Kerberos-based security has been added to NFSv4.
FTPS support	FTP over SSL/TLS is available.
NetVault v8 support	Support has been added for NetVault v8.2.
Filesystem Check	The WebUI now provides the ability to check filesystems for errors and repair those errors, if stipulated.
Server Cloning (via Disaster Recovery)	The configuration of one server can now be applied to a different server using the Disaster Recovery backup and restore system.
Multi-server Administration with SnapServer Manager	SnapServer Manager can now manage administrative tasks on multiple SnapServers at the same time.

What's New in GuardianOS v5.0

GuardianOS 5.0 has the following new features and functionality

Feature	New Functionality
Improved system performance	Improved memory management, resulting in reduced swap utilization, which improves overall performance of the operating system.
Enhanced Windows security and permissions compatibility	File system access control lists (ACL) now follow the Windows NTFS security paradigm for assignment and enforcement of file system permissions.
Improved User Interface	Updated Storage UI improves ease of configuration of storage resources.
RAID 6 and RAID 10 support	Two new RAID configuration options are available: • RAID 6 provides a dual parity RAID for additional redundancy and data protection. • RAID 10 stripes RAID 1 mirrors for high data protection and increased performance.
NFS v4 support	Support for NFS v4 has been added, providing a connection-based protocol for NFS users, with elimination of ancillary protocols, single port accessibility, new file system view, and improved network management. **Note** Kerberos-based security and NFS v4 ACLs are not supported in this release of GuardianOS.
Expanded CLI	Over 30 additional commands have been incorporated into the SnapCLI, increasing the ability to perform configuration tasks using the CLI or CLI scripts.
Dynamic Home Directories	With Home Directories enabled, users are provided with their own private directory and (for SMB, AFP, NFS, and HTTP) user-specific share, to which only they and the system administrator have access.
Switch-side Load Balancing	Two additional Load Balancing options have been added. Switch Trunking and Link Aggregation group multiple physical Ethernet links to create one logical interface, providing high fault tolerance and fast performance between switches, routers, and servers.
NTP Server	The SnapServer can now act as an NTP Server to provide synchronization to other SnapServers or NTP clients.
Expanded iSCSI capabilities	Additional support for MPIO has been added, as well as support for Microsoft's DSM module and Microsoft Cluster Services.

What's New in GuardianOS v4.4

GuardianOS 4.4 has the following new features and functionality

Feature	New Functionality
Data Migration utility	Utility that allows you to migrate data from any server or workstation supporting CIFS or NFS to a SnapServer.
Command Line Interface	Support for performing certain GuardianOS functions using a command line shell rather than the GUI.
Enhanced Disaster Recovery	Support for recovering Snap EDR Management Console settings if EDR was backed up as part of the Disaster Recovery Image.
Enhanced iSCSI support	Increased support for iSCSI targets and support for spec-compliant IQN names.
New OS and browser support	Support has been added for Windows Vista, Internet Explorer 7, and FireFox 1.5 and 2.0.
USB tape drive support	Attach backup tape devices using USB 2.0 as well as SCSI connections.
Improved share name support	Share names can now be 27 characters long and can include spaces.
USB Print Server capability	Multiple printers can be connected via USB ports to the SnapServer, which can be configured to emulate a Windows or IPP print server.
Ethernet Port disabling	Unused ethernet2 ports can now be disabled.
Windows Domain Authentication for Mac users	AFP users can now authenticate as domain users. They no longer require local user accounts to access a SnapServer joined to a Windows NT or Active Directory domain.
Mac OSX clients can connect via SMB	Support for Mac OSX clients to connect to Microsoft networking as well as AFP. Mac OS9 and earlier users must still connect using AFP.
Automatic Adjustment for U.S. Daylight Saving Time	GuardianOS automatically adjusts for the new U.S. Daylight Saving Time schedule, depending on your time zone.
New Time Zones	New time zones are dedicated to Mexico, as Mexico is not following the new U.S. Daylight Saving Time schedule.

What's New in GuardianOS v4.3/4.2

GuardianOS 4.3/4.2 contains the following new functionality:

Feature	New Functionality
Enhanced NFS client support in Unicode mode	Additional NFS client code page option for UTF-8 in Unicode mode, supporting the default client character set of many Linux/Unix distributions..
Upgrade of NetVault Bakbone	NetVault Bakbone has been upgraded from v7.1.1 to v7.4
Improved Snap EDR support	Snap EDR is now pre-installed at the factory.
Improved UPS support	Additional support for UPS devices includes: • Support for APC-branded USB UPS devices. • New option to restart the server when power is restored.
Improved Quotas design	The Quotas pages have been redesigned to simplify adding quotas for users and groups and to enhance usability.
Auto-refresh feature	An auto-refresh selection has been added to the Home page. When selected, the server status is automatically updated at 45 or 90 second intervals.

What's New in GuardianOS v4.1

GuardianOS v4.1 introduced the following new functionality:

Feature (pre-4.1)	New (4.1) Functionality
RAID Sets	The RAID Sets page contains a **RAID Settings** button that opens the new RAID Settings page. This page has options for two new features: • **Background disk scan.** When this feature is enabled, a disk scrubber runs in the background and continuously scans disk drives for media errors. • **Automatic incorporation of unused disks into degraded RAIDs.** When this feature is enabled, raw disks or unconfigured GuardianOS-partitioned disks will be automatically incorporated into degraded RAID 5 or RAID 1 sets upon hot-insertion.
System Monitoring	The System Monitoring page now contains RAID status information for each of the RAID sets.

What's New in GuardianOS v4.0

Note Starting with GuardianOS v4.0, Backup Express is no longer supported.

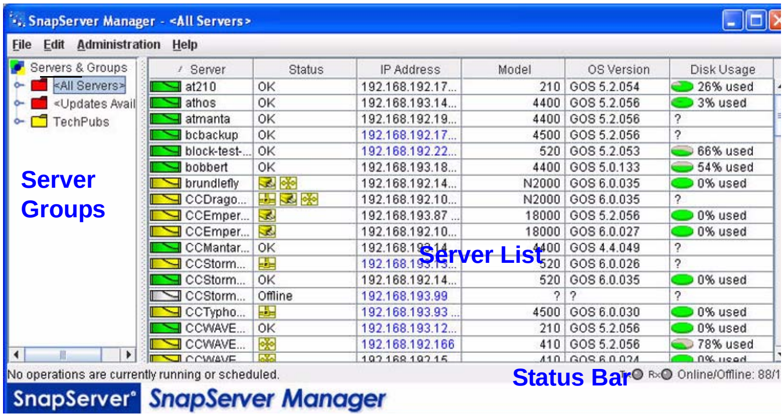
GuardianOS v4.0 introduced the following notable changes to the web admnistration interface:

Feature (pre-4.0)	New (4.0) Functionality
Add-on Features	Add-on and 3rd-party features are now managed together on the **SnapExtensions** page, accessible from the home page's Site Map or by clicking the SnapExtensions icon in the upper right corner of the Administration tool.
Changing the Admin User Password	Local users, including the admin user, are managed from the **Security > Local Users** page. Select the admin user from the user list and click **Properties** to change the password.
Windows Networking	Windows networking settings, including domain joining, are now located on a single page, **Network > Windows**.
View all disks (formerly from Storage > Devices page)	The new **Storage > Disks/Units** page displays a graphical view of all disks for the head unit as well as for any attached expansion units, allowing you to move your mouse over a disk to highlight all of the disks in a particular RAID set.
Share Management	Share creation, modification, and access privileges are now all managed from a single page, **Security > Shares**. Also, the process of assigning user and group access to a share has been greatly improved.

SnapServer Manager

SnapServer Manager (SSM) is a Java-based, platform-independent, multiserver administrative application that runs on all major platforms. SSM provides a single interface from which administrators can discover, configure, and monitor all GuardianOS SnapServers on their network. With SSM, administrators can compare, copy, and configure settings for groups of GuardianOS SnapServers in a single operation.

Right-click a server group to administer multiple servers at the same time



Server	Status	IP Address	Model	OS Version	Disk Usage
at210	OK	192.168.192.17...	210	GOS 5.2.054	26% used
athos	OK	192.168.193.14...	4400	GOS 5.2.056	3% used
atmanta	OK	192.168.192.19...	4400	GOS 5.2.056	?
bcbackup	OK	192.168.192.17...	4500	GOS 5.2.056	?
block-test-...	OK	192.168.192.22...	520	GOS 5.2.053	66% used
bobbert	OK	192.168.193.18...	4400	GOS 5.0.133	54% used
brundlefly		192.168.192.14...	N2000	GOS 6.0.035	0% used
CCDrago...		192.168.192.10...	N2000	GOS 6.0.035	?
CCEmper...		192.168.193.87 ...	18000	GOS 5.2.056	0% used
CCEmper...		192.168.192.10...	18000	GOS 6.0.027	0% used
CCMantar...	OK	192.168.192.14...	4400	GOS 4.4.049	?
CCStorm...		192.168.193.13...	520	GOS 6.0.026	?
CCStorm...	OK	192.168.192.14...	520	GOS 6.0.035	0% used
CCStorm...	Offline	192.168.193.99	?	?	?
CCTypho...		192.168.193.93 ...	4500	GOS 6.0.030	0% used
CCWAVE...	OK	192.168.193.12...	210	GOS 5.2.056	0% used
CCWAVE...		192.168.192.166	410	GOS 5.2.056	78% used
CCWAVE		192.168.192.15	410	GOS 6.0.024	0% used

No operations are currently running or scheduled.

Tx Rx Online/Offline: 88/1

Installing SSM

You can download and install SSM using the *SnapServerToolsInstall.html* file found on your SnapServer User CD. SSM can be installed to all client platforms, including Windows, Macintosh OS X, Linux, and UNIX.

If you plan to run SSM on a Macintosh client, you must upgrade the client to MacOS 10.2 or higher (required for JRE 1.4.0 or higher support).

Launching SnapServer Manager

Launch SSM using one of the methods described in the following table:

Operating System	Procedure
Microsoft Windows NT/XP/ 2000/2003/Vista/2008/7	Click **Start**. Point to **Programs** (or **All Programs**)**>** SnapServer Manager, then select SnapServer Manager.
Macintosh v10.2 or higher	Open the SnapServer Manager folder and double-click the SnapServer Manager icon.
UNIX/Linux	For default options: cd to home directory, then run the SnapServer Manager command: **`./Snap_Server_Manager`** If you selected not to create links: cd to home directory, then cd to the SnapServer Manager directory, and run the SnapServer Manager command: **`./Snap_Server_Manager`**

Multiserver Administration

Multiserver administration is available only for GuardianOS SnapServers.

- **Simultaneous application of settings to server groups —** You can organize GuardianOS servers into functional groups and apply settings to all servers in the group simultaneously.
- **Comparing settings across servers —** SSM can compare settings across any number of GuardianOS servers and identify when settings differ among servers. For example, comparing protocol access configuration for a group of servers may reveal that settings are consistent for Windows, NFS, and AFP but that differences exist among servers in HTTP/HTTPS and FTP/FTPS settings.
- **Copying settings from one server to one or more different servers —** SSM can copy selected settings (TCP/IP, SNMP, SMB, etc.) from any GuardianOS server to one or more different GuardianOS servers.
- **Scheduling operations to run during offpeak hours —** Operations can be scheduled to run on multiple GuardianOS servers during offpeak hours.
- **Automatic email notification of completed operations —** You can configure SSM to send an operations report (CSV format) upon completion of any operation.
- **Automatic notification of available GuardianOS updates —** SSM is by default configured to check daily for applicable updates to the servers it has discovered and display an alert, notifying the administrator of the available updates.

SSM Feature Licensing

Use the SSM Feature Licensing menu to apply SnapExtension license keys to one or more servers. There is no limit to the number of licenses that can be entered using this dialogue box.

1 Start SSM and select the GuardianOS servers to be licensed.

2 Navigate to **Administration > Feature Licensing**. If you have not already obtained your licenses, in the License Required dialog box, select **Click here to purchase SnapExtension license keys at www.snapserver.com**.

3 Once you have obtained the license keys, enter one license key per line (or multiple keys per line, separated by spaces), click **Enter License...**, then click **OK**.

Note This feature is only available for servers running GuardianOS v 4.0 or later.

The Feature License dialogue box does not display any pre-existing SnapExtension licenses. Only licenses that have been applied while the current dialogue box is open will be displayed.

Connecting to the Server for the First Time

SnapServers are preset to acquire an IP address from a DHCP server. If no DHCP server is found on the network, the SnapServer defaults to an IP address of 10.10.10.10, and you may not be able to see the server on your network. You can discover a SnapServer using either the default server name or the SSM utility. Use the server name method if you are installing one SnapServer on the network. Use SSM if you are installing two or more SnapServers, or if your network does not have IP to name resolution services.

To Connect Using the Server Name

This procedure requires that name resolution services (via Windows Internet Naming Service [WINS] or Domain Name System [DNS]) be operational.

1 **Find the server name.**

For SnapServers 510, 520, 550, 620, 650, and 18000, you can read the server name and IP address on the LCD panel.

For the SnapServers 110, 210, 410, N2000, 4200, and 4500, use the default server name of SNAP*nnnnnn,* where *nnnnnn* is the server number. For example, the name of a SnapServer with a server number of 610019 is SNAP610019.

The server number is a unique, numeric-only string that appears on a label affixed to the chassis.

- On the SnapServer 410 and N2000, the server label is located on the top of the chassis in the left front corner.
- On the SnapServer 110 or 210, the label is on the underside of the chassis.
- To obtain the server number for SnapServer 4200 and 4500, remove the front bezel to read the label.

2 **Connect to the server.**

In a Web browser, enter the following URL:

`http://SNAP`*`nnnnnn`* (where *nnnnnn* is the server number)

Press Enter. The Web View screen opens.

3 **Log into the Administration Tool.**

Click the **administration** link, and in the login dialog box, enter *admin* as the user name and *admin* as the password, and then click **OK**.

4 **Complete the Initial Setup Wizard.**

For instructions for using the Initial Setup Wizard, see page 16.

To Connect to a SnapServer Using SSM

1 **Install and launch SnapServer Manager.**

Install and launch SSM (see page 12) on a machine residing on the same network segment as your SnapServer(s). Upon startup, SSM displays the IP address of each SnapServer on its local network segment.

2 **If using a DHCP server, skip to the next step. Otherwise:**

In the SSM console, right-click a server name and select **Set IP Address**. At a minimum, enter an IP address for the SnapServer and a subnet mask, and then click **OK**.

3 **Launch the Administration Tool from the SSM console.**

In the SSM console, right-click a server name and select **Launch Web Administration**.

4 **Log into the Administration Tool.**

Click the **Administration** link, and in the login dialog box, enter *admin* as the user name and *admin* as the password, and then click **OK**.

5 **Complete the Initial Setup Wizard.**

For instructions for using the Initial Setup Wizard, see the next section.

Using the Initial Setup Wizard

The first time you connect to a SnapServer via the browser-based Administration Tool, the Initial Setup Wizard runs. The Initial Setup Wizard consists of several screens that allow you to change the server name, set the date and time, set the administrator password, configure TCP/IP settings for the primary Ethernet port (by default Ethernet1), and reclaim the snapshot space that is by default allotted on the volume.

Server Name

The default server name is SNAP*nnnnnn*, where *nnnnnn* is the server number. If desired, enter a unique server name of up to 15 alphanumeric characters. In addition to letters and numbers, you can also use a dash (-) between characters, but spaces are not allowed.

Date/Time Settings

The SnapServer time stamp applies when recording server activity in the event log (Monitor Menu), setting the create/modify time on a file, and when scheduling snapshot, antivirus, Snap EDR, or Server-to-Server Synchronization (pre-GuardianOS v4.2 licenses only) operations. Edit the settings according to local conditions.

Note GuardianOS automatically adjusts for Daylight Saving Time, based on the selected time zone.

Changing the Administration Password

The default administrator user name is *admin* and the default password is also *admin*. To prevent unauthorized access to the SnapServer, enter a secure password immediately in the fields provided.

Note A password must consist of 1 to 15 alphanumeric characters and is case sensitive.

Gathering TCP/IP Addressing Information

SnapServers are preset to acquire an IP address from a DHCP server. If you wish to assign a static IP instead, assemble the following information:

- The IP address for the SnapServer (required)
- The subnet mask (required)

- The default gateway IP address
- The DNS IP address
- WINS server(s) IP address(es)

Keeping or Reclaiming the Snapshot Space

A Snapshot is a point-in-time image of your volume. This image can be used for backup or recovery purposes. See "Snapshots" on page 111 for detailed information. Approximately 20% of the default volume is allocated for snapshot use.

If you are certain that you will not use snapshots, you can reclaim that space on the volume by selecting the **Reclaim Snapshot Space** radio button in the Initial Setup Wizard.

Caution If you delete the snapshot space at this time (during the volume configuration process), you will not be able to restore it later if you decide that you want to use snapshots. Therefore, it is recommended that you retain the snapshot space during this initial configuration. You can always delete or reduce it from the **Storage > Snapshots** page in the Administration Tool. Or, for servers with no Snapshots license, you can simply increase your default volume size in the **Storage > Volumes** page.

Determining Capacity

The factory default configuration reduces potential capacity in order to provide a high degree of data protection and backup capability. By default, SnapServers with four (4) to eight (8) disk drives are configured into a RAID 5 created during the manufacturing process. SnapServers with twelve (12) disk drives are configured into a RAID 6, and the SnapServer 110 and SnapServer 210 are configured as a 1- and 2-drive RAID 0, respectively. In a RAID 5 configuration, the capacity of one drive is used for data protection, reducing the available capacity of the server by one drive. In a RAID 6 configuration, where two drives are used for data protection, the available drive capacity of the server is reduced by two.

The GuardianOS runs from a protected partition, which consumes approximately 1 GB of space from each disk depending on the total capacity of the disk drive. Approximately 20% of the default RAID is available for snapshot space and 80% of the default RAID assigned to the primary data volume.

For example, to calculate the capacity of a SnapServer 520 with 1 TB total capacity in its default state, consider both the hardware and software configuration:

- The four 250 GB disk drives each provide 240 GB of formatted capacity.
- The four disks when joined in a RAID 5 configuration net 720 GB of capacity for the RAID.
- The snapshot space is 20% of the space available on the RAID, reducing the space on the RAID for the data volume by 144 GB.

Scheduling Data Protection Tasks

Note For some SnapServers, additional licenses are required for NetVault, SnapEDR, and antivirus functionality.

Scheduling backups, snapshots, and antivirus scans, and creating a disaster recovery image preserves your server configuration and protects your data from loss or corruption. Snapshots can be taken to provide a point-in-time image of files and changes to files to help in quickly recovering from accidental deletion or modification, or to facilitate performing an offline tape backup of an active data partition.

Navigate to **Storage > Snapshots** in the browser-based Administration Tool to schedule snapshots or modify the space available for storing snapshots. Snapshots should be taken when the system is idle or under low data traffic.

Set up antivirus protection by clicking the **SnapExtensions** icon, and then clicking **CA Antivirus.** Click the checkbox to enable antivirus, and click **OK.** When the configuration link appears, click it to launch the *e*Trust administration user interface for configuration and scheduling of virus scans and virus signature file updates.

Create a disaster recovery image (DRImage) on the **Maintenance > Disaster Recovery** page. This DRImage should be created after the server configuration is complete, and can be used to recover the server or a replacement server to the configured state. See "Disaster Recovery" on page 117 for detailed information on creating and using disaster recovery images.

GuardianOS contains built-in support for BakBone Netvault to back up to a local tape and for SnapEDR to synchronize and back up to and from other SnapServers. GuardianOS also supports several third-party backup agents. For information on using these backup methods to help protect your data, see "Backup and Replication Solutions" on page 147.

Migrating Data from Legacy Servers to the SnapServer

The Data Migration utility can be used to copy or move data from any computer supporting CIFS/SMB or NFS (v2 and v3) directly to a SnapServer. Access the utility by selecting **Maintenance > Data Migration**. For more information, see "Data Migration" on page 61.

Configuring the SnapServer as a Print Server

Your SnapServer can be configured to emulate either a Windows or an IPP print server to manage USB-connected printers. To configure your SnapServer as a print server, select **Server > Printing** in the Administration Tool. For more information, see "Print Server" on page 39.

Configuring the SnapServer as a Simple Web Server

When the SnapServer is configured with a web root, the browser opens to a user-definable directory and optionally automatically loads a default HTML page when a user connects with a web browser to the root of the server (e.g., `http://[servername]` or `http://[ipaddress]`). To configure a web root on the SnapServer, select **Network > Web** in the Administration Tool. For more information, see "Using WebRoot to Configure the SnapServer as a Simple Web Server" on page 37.

Configuring an APC-Brand UPS

Overland Storage recommends that you use a UPS with SnapServers and expansion arrays to protect your data from unforeseen power outages. SnapServers are compatible with USB- and network-based, APC-brand uninterruptible power supplies that allow you to take advantage of the automatic shutdown capability (some serial-only APC UPS's are also supported by using the IOGear GUC232A USB to Serial Adapter Cable). For instructions on configuring your APC-brand UPS device, navigate to the **Server > UPS** screen and click the **Help** icon.

Note The SnapServer 14000 supports a network-based UPS only.

SnapExtensions

SnapExtensions are software applications, agents, and utilities that extend the capabilities of a SnapServer. Some SnapExtensions are fully functional out-of-the-box; others may require a download and/or the purchase of a license for full operation. For up-to-date information on feature availability, contact Overland Storage.

To access SnapExtensions, click the SnapExtensions icon from any page in the administration web UI.

You may have a different set of SnapExtensions available to you than are listed in the following table if you have installed other SnapServer software, independent of the current operating system release.

Feature	Description
CA *e*Trust Antivirus	Preinstalled antivirus software that is fully functional out-of-the-box. For information on configuring the software, see "CA eTrust Antivirus Software" on page 125. **Note** A separate license is required on some platforms.
BakBone NetVault	Preinstalled backup software (GuardianOS v3.0 & later) with a Workgroup Server license. For information on installing and configuring NetVault, see "BakBone Netvault" on page 148, and the documentation included with the NetVault CD that shipped with your SnapServer. **Note** A separate license is required on some platforms.
Snap EDR Management Console and Agent	Utility included with your SnapServer that synchronizes, transfers, backs up, and restores files between Windows, UNIX, and GuardianOS systems. Comes with a 45 day trial license, but requires a license for each SnapServer thereafter. For more information, see "Snap Enterprise Data Replicator (Snap EDR)" on page 149.

Wake-on-LAN Support

Note Available on SnapServer NAS N2000 only.

Wake-on-LAN, the Ethernet computer networking standard that allows a powered-off computer to be powered on by a network signal, is automatically enabled (and cannot be disabled) for Ethernet 1 and Ethernet 2. Wake-on-LAN is activated when another computer on the same LAN sends a “magic packet” to the SnapServer using a program designed to send magic packets.

Network Access to the Server

SnapServers are preconfigured to use DHCP, autonegotiate network settings, and allow access to the server for Windows (CIFS/SMB), Unix (NFS), Macintosh (AFP), FTP/FTPS, and HTTP/HTTPS clients. Discussed next are the options for configuring TCP/IP addressing, network bonding, and access protocols. Network bonding options allow you to configure the SnapServer for load balancing and failover. Network protocols control which network clients can access the server.

Topics in Network Access:

- TCP/IP Options
- Configuring TCP/IP Settings
- Default Network Protocol Settings
- Windows Networking Configuration
- NFS Access
- Apple Networking Configuration
- FTP/FTPS Access
- HTTP/HTTPS Access
- DHCP Server
- Print Server

Note The default settings enable access to the SnapServer via all protocols supported by the SnapServer. As a security measure, disable all protocols not in use. For example, if no Macintosh or FTP clients need access to the SnapServer, disable these protocols in the Administration Tool.

Viewing Current Network Settings

The **Network > Information** screen displays the server's current network settings. One column appears for each Ethernet port. Field definitions are given in the following table:

Ethernet Interface Information	
Port Name	The name of the ethernet interface (e.g., Ethernet1)
Enabled	Yes or no
TCP/IP Settings Obtained from	DHCP or Static
IP Address	The unique 32-bit value that identifies the server on a network subnet. This address consists of a network address, optional subnet address, and host address. It displays as four addresses ranging from 1 to 255, separated by periods (.).
Subnet Mask	A portion of a network that shares a common address component. On TCP/IP networks, subnets are all devices with IP addresses that have the same prefix.
Primary WINS Server	The Windows Internet Naming Service server, which locates network resources in a TCP/IP-based Windows network by automatically configuring and maintaining the name and IP address mapping tables.
Secondary WINS Servers	Secondary Windows Internet Naming Service server(s)
Ethernet Address	The unique six-digit hexadecimal (0-9, A-F) number that identifies the Ethernet port
Speed Status	10 Mbps, 100 Mbps, or 1000 Mbps
Duplex Status	Half-duplex: two-way data flow, only one way at a time. Full-duplex: two-way data flow simultaneously.
Bonding Status	Standalone, Load balance, Failover, Switch Trunking, or Link Aggregation

Gateway Information	
Default Gateway	The network address of the gateway is the hardware or software that bridges the gap between two otherwise unroutable networks. It allows data to be transferred among computers that are on different subnets.

DNS Information	
Domain Name	The ASCII name that identifies the internet domain for a group of computers within a network.
Primary DNS	The IP address of the primary Domain Name System server that maintains the list of all host names.
Secondary DNS #1	Secondary Domain Name System server #1
Secondary DNS #2	Secondary Domain Name System server #2

TCP/IP Options

GuardianOS SnapServers ship with one or more Gigabit Ethernet (GbE) ports.

The following table describes TCP/IP options; default settings appear in italics.

Option	Setting	Description
TCP/IP Addressing	*DHCP*	By default, SnapServers acquire an IP address from the DHCP server on the network.
	Static	Administrators may assign a fixed IP address or other IP settings as necessary.
Network bonding Note Only applicable to servers with more than one ethernet port.	*Standalone*	The default *Standalone* setting treats each port as a separate interface, effectively disabling network bonding. Network bonding treats two or more ports as a single channel for failover or load balancing purposes.
	Load Balance (ALB)	An intelligent software adaptive agent repeatedly analyzes the traffic flow from the server and distributes the packets based on destination addresses, evenly distributing network traffic for optimal network performance. All ports in the same ALB configuration need to be connected to the same switch.
	Failover	This mode uses one Ethernet port (by default Ethernet1) as the primary network interface and one or more Ethernet ports are held in reserve as backup interfaces. Redundant network interfaces ensure that an active port is available at all times. If the primary port fails due to a hardware or cable problem, one of the backup ports assumes its network identity. The ports should be connected to different switches (though this is not required). Note Failover mode provides switch fault tolerance, as long as the ports are connected to different switches.

Option	Setting	Description
	Switch Trunking	This mode groups multiple physical Ethernet links to create one logical interface. Provides high fault tolerance and fast performance between switches, routers, and servers.
	Link Aggregation (802.3ad)	Like Switch Trunking, this mode groups multiple physical Ethernet interfaces to create one logical interface, and provides high fault tolerance and fast performance between switches, routers, and servers. Uses Link Aggregation Control Protocol (LACP) to autonegotiate trunk settings.
Enable Ethernet	*Checked*	By default, all Ethernet ports are enabled, whether they are used or not.
	Unchecked	Ports other than the Primary Interface (by default Ethernet1) can be disabled by selecting the port and unchecking the Enable Ethernet checkbox. However, a bonded Ethernet port cannot be disabled, nor can a disabled Ethernet port be placed in bonded mode. **Note** The primary Ethernet port must always be enabled. GuardianOS will not allow you to disable it.
Speed/ duplex	*Auto*	The default setting of *Auto* enables automatic negotiation of the speed and duplex settings based on the physical port connection to a switch. The speed setting establishes the rate of transmission and reception of data. The duplex setting allows the Ethernet port to transmit and receive network packets simultaneously. **Note** Auto is the only allowable setting for a Gigabit port.
	Fixed	The SnapServer may also be set to fixed speed/duplex setting: 10Mbps/half; 10Mbps/full; 100Mbps/half; 100Mbps/full **Note** To prevent connectivity problems when changing to a fixed setting, see “Changing from Auto to a Fixed Setting” on page 27.
Primary Interface		By default, the primary Ethernet port is Ethernet1 and it cannot be disabled. However, the Primary Interface can be changed to a different Ethernet port by selecting the Ethernet port you want to make Primary and putting a check in the Primary Interface box. The Primary Interface is prioritized for various network configuration parameters that apply to the server as a whole (e.g., DNS IP address, hostname, and default gateway). In addition, the IP address of the Primary Interface is preferred to identify the server for various services and circumstances that require a single IP address.

Configuring TCP/IP Settings

TCP/IP settings are configured on the **Network > TCP/IP** screen of the Administration Tool. This screen displays information about the server's Ethernet ports, including:

Column	Description
Port/Bond	A list of the Ethernet Ports or Bonds. Click a port or bond to display or modify configuration details.
Status	• *OK*—Port is connected and active. • *No link*—Port is not connected • *Failed*—Port has failed
IP Address	• The IP address for the NIC or bond if known or *not available* if unknown. • Whether the IP address was obtained by *DHCP* or is *Static*.
Bond Type	• *Standalone*—The default *Standalone* setting treats each port as a separate interface, effectively disabling network bonding. Network bonding treats two or more ports as a single channel for failover or load balancing purposes.
	• *Load Balance (ALB)*—An intelligent software adaptive agent repeatedly analyzes the traffic flow from the server and distributes the packets based on destination addresses, evenly distributing network traffic for optimal network performance. All ports in the same ALB configuration need to be connected to the same switch.
	• *Failover*—This mode uses one Ethernet port (by default Ethernet1) as the primary network interface and a second or more Ethernet ports are held in reserve as the backup interface. Redundant network interfaces ensure that an active port is available at all times. If the primary port fails due to a hardware or cable problem, the second port assumes its network identity. The ports should be connected to different switches (though this is not required). **Note** Failover mode provides switch fault tolerance, as long as ports are connected to different switches.
	• *Switch Trunking*—This mode groups multiple physical Ethernet links to create one logical interface. Provides high fault tolerance and fast performance between switches, routers, and servers.

Column	Description
	• *Link Aggregation (802.3ad)*—Like Switch Trunking, this mode groups multiple physical Ethernet interfaces to create one logical interface, and provides high fault tolerance and fast performance between switches, routers, and servers. Uses Link Aggregation Control Protocol (LACP) to autonegotiate trunk settings.
Modified	Indicates whether configuration for one or more interfaces has been changed and needs to be applied to take effect: • *Yes*—One or more parameters for the interface have been modified. • *No*—No parameters for the interface have been modified.

Issues in TCP/IP Configuration

Consider the following guidelines when connecting a SnapServer to the network.

Cabling for Single-Subnet, Multihomed, or Network Bonding Configurations

- **For a Single Subnet or Multihomed Configuration (Standalone) —** Standalone treats each port as a separate interface. In a single-subnet configuration, only the primary port is connected to the switch. In a multihomed configuration, each port is cabled to a different switch and the network connections lead to separate subnets.

  Caution Do not connect multiple Ethernet ports to the same network segment in Standalone mode, except for iSCSI MPIO configurations. This configuration is not supported by most network file protocols and can lead to unexpected results.

  Caution If you connect only one port, use the primary port (Ethernet1). If you use Ethernet2, some services may not function properly.

- **For a Network Bonding Configuration (Load Balancing, Failover, Switch Trunking, or Link Aggregation) —** Network bonding technology treats multiple ports as a single channel, with the network using one IP address for the server.

  Note This network bonding configuration is only applicable to SnapServers with more than one ethernet port.

  To take advantage of network bonding, all ports in the bonded team must be physically connected to the same network:

  - For load balancing, Switch Trunking, or Link Aggregation, connected to the same switch on the same subnet; or
  - For failover, connected to a different switch on the same subnet (in case one switch fails).

Connect the SnapServer to the Network via a Switch

While it is possible to connect a SnapServer to the network via a hub, this configuration unduly restricts the performance of the server for the following reasons:

- Hubs do not support full-duplex. You can employ full-duplex only when the SnapServer is connected to a switch.
- Hubs do not support Gigabit speeds. Attempting to force a Gigabit setting when the SnapServer is cabled to a hub will produce unintended consequences.

100 Mps/half duplex is the best performance possible when connected to a hub.

Make Sure the Switch is Set to Autonegotiate Speed/Duplex Settings

When the server is shipped from the factory, both ports are set to autonegotiate. This setting allows the SnapServer to base speed and duplex settings on the physical port connection to a switch. Thus, the switch/hub to which the SnapServer is cabled *must* be set to autonegotiate to initially connect to the server; otherwise, network throughput or connectivity to the server may be seriously impacted.

To use fixed duplex settings (not applicable to gigabit), the same fixed setting must be set on the server and switch.

Configure the Switch for Load Balancing

If you select either the Switch Trunking or Link Aggregation network bonding configuration, be sure the switch is configured correctly for that bonding method. No switch configuration is required for Adaptive Load Balancing (ALB).

Changing from Auto to a Fixed Setting

You can configure a fixed setting on the **Network > TCP/IP** screen in the browser-based Administration Tool. If you change this setting, be sure to:

- Configure the fixed setting in the Administration Tool first; and
- Configure the switch to the same fixed setting.

If you change the switch setting before you change the setting in the Administration Tool, the SnapServer may not connect to the network. The **Link** LED on the SnapServer front panel will be off or amber if the server is not connected to the network.

> **Note** AppleTalk (disabled by default) cannot be enabled when one or more Switch Trunking of Link Aggregation configurations exist.

Default Network Protocol Settings

SnapServers are preconfigured to allow multiplatform access in heterogeneous Windows, UNIX/Linux, and Macintosh environments. The following table summarizes the SnapServer's default network protocol access configuration.

Protocol	Default	Comments
Windows (CIFS/ SMB)	Enabled	Allows access to Windows clients via the workgroup *Workgroup*.
UNIX (NFS)	Enabled	Allows universal access to all computers running NFS without client address restrictions.
Apple (AFP)	Enabled	Allows access over an AppleTalk or TCP/IP network using the default zone.
FTP/FTPS	Enabled for FTP, FTPS, and Anonymous User	• Allows users to access files via FTP or FTPS. • Allows access using the anonymous user account, which is mapped to the SnapServer's local guest user account.
HTTP/HTTPS (Internet/Intranet)	Enabled	Allows users to access files via HTTP or HTTPS using a Web browser.
DHCP Server	Disabled	Allows SnapServers to distribute IP addresses to network clients.
Secure Shell (SSH)	Enabled	Required when installing a supported backup agent, using the Command Line Interface, or troubleshooting under the direction of a technical support representative. Using SSH for any other purpose is not supported and may void your warranty.

Note As a security measure, disable any network protocols not required in your network environment.

Windows Networking Configuration

Windows SMB and security settings are configured on the **Network > Windows** screen of the Administration Tool.

Topics include:

- Support for Windows Networking (SMB)
- Support for Windows Network Authentication

Support for Windows Networking (SMB)

The default settings make the SnapServer available to SMB clients in the workgroup named *Workgroup*. Language support is set to North America/Europe (code page 850); opportunistic locking is enabled, as is participation in master browser elections. See the online help for details in configuring these options.

Consider the following when configuring access for your Windows networking clients.

Windows Networking File and Folder Name Support

In Windows networking, most file and directory names are transmitted as a 2-byte (16-bit) UCS-2 character set. However, this is not true in every case. Some are still sent via a single byte character set. The Language Support option selected for Windows networking clients is used only to enable the server to accept file and folder names in a single byte character set.

Caution When Unicode is disabled, do not name files and folders in character sets not included in this list (e.g., Cyrillic). Such files and folders may be impossible to open or delete.

Support for Microsoft Name Resolution Servers

The SnapServer supports both of the Microsoft name resolution services: Windows Internet Naming Service (WINS) and Dynamic Domain Name System (DDNS). However, when you use a domain name server with a Windows Active Directory (ADS) server, make sure the forward and reverse name lookup is correctly set up. ADS can use a UNIX BIND server for DNS as well.

ShareName$ Support

GuardianOS supports appending the dollar-sign character ($) to the name of a share in order to hide the share from SMB clients accessing the SnapServer.

Note As with Windows servers, shares ending in '$' are not truly hidden, but rather are filtered out by the Windows client. As a result, some clients and protocols can still see these shares. To completely hide shares from visibility from any protocols, the **Security > Shares** screen gives you access to a separate and distinct Hidden share option that hides a share from SMB, AFP, HTTP, HTTPS, and FTP clients (However, shares are not hidden from NFS clients, which cannot connect to shares that aren't visible. To hide shares from NFS clients, consider disabling NFS access on hidden shares). For new shares, select **Create Share** and click the **Advanced Share Properties** button to access the Hidden share option. For existing shares, select the share, click **Properties**, and click **Advanced Share Properties** to access the Hidden share option.

Support for Windows Network Authentication

This section summarizes important facts regarding the GuardianOS implementation of Windows network authentication.

Windows Networking Options

Windows networks use a domain controller to store user credentials. The domain controller can validate all authentication requests on behalf of other systems in the domain.

Option	Description
Workgroup	In a workgroup environment, users and groups are stored and managed separately on each server in the workgroup.
Domain (NT or ADS)	When operating in a Windows NT or Active Directory domain environment, the SnapServer is a member of the domain and the domain controller is the repository of all account information. Client machines are also members of the domain and users log into the domain through their Windows-based client machines. Windows or Active Directory domains resolve user authentication and group membership through the domain controller. Once joined to a Windows NT or Active Directory domain, the SnapServer imports and then maintains a current list of the users and groups on the domain. Thus, you must use the domain controller to make modifications to user or group accounts. Changes you make on the domain controller appear automatically on the SnapServer. **Note** Windows 2000 domain controllers must run SP2 or later.

Kerberos Authentication

Kerberos is a secure method for authenticating a request for a service in a network. Kerberos lets a user request an encrypted "ticket" from an authentication process that can then be used to request a service from a server. The user credentials are always encrypted before they are transmitted over the network.

The SnapServer supports the Microsoft Windows implementation of Kerberos. In Windows Active Directory (ADS), the domain controller is also the directory server, the Kerberos key distribution center (KDC), and the origin of group policies that are applied to the domain.

Notes Kerberos requires the server's time to be closely synchronized to the domain controller's time. This means that (1) the server automatically synchronizes its time to the domain controller's and (2) NTP cannot be enabled when joined to an ADS domain.

Interoperability with Active Directory Authentication

The SnapServer supports the Microsoft Windows 2000/2003/2008 family of servers that run in native ADS mode or in mixed NT/ADS mode. SnapServers can join Active Directory domains as member servers. References to the SnapServer's shares can be added to organizational units (OU) as shared folder objects.

Note Windows 2000 domain controllers must run SP2 or later.

Guest Account Access to the SnapServer

The **Security > Local Users** screen contains an option that allows unknown users to access the SnapServer using the guest account.

Restrict_Anonymous and PDC Access

If you have implemented the *restrict_anonymous* mechanism on your domain, you may need to enter a valid domain (not local) user name and password that the SnapServer can use to communicate with the PDC. For ease of administration, Overland Storage recommends that you create a unique user account on the domain using the following guidelines:

- Choose a name, such as *SnapServerAccess*, and include a comment that makes the function of the account clear.
- Set the password to never expire.

Note A *restrict_anonymous* user account does not require administrative access.

Connecting from a Windows Client

Windows clients can connect to the SnapServer using either the server name or IP address. To navigate to the server using Windows Explorer, use one of these procedures:

- For Microsoft Windows Vista, 2008, and 7 clients, navigate to **Network >** *server_name*.
- For Microsoft Windows 2003, 2000, Me, or XP clients, navigate to **My Network Places >** *workgroup_name* > *server_name* .
- For Microsoft Windows 95, 98, or NT clients, navigate to **Network Neighborhood >** *workgroup_name* > *server_name.*

Mapping a Drive in Windows

In addition to browsing the network to find the SnapServer and access its shares, you can also connect to your SnapServer by mapping a drive to a share on the server. The procedure to map a drive is essentially the same for all versions of Windows, though some of the names change slightly from version to version (e.g., My Computer in NT/2000/XP vs Computer in Vista).

1 Right-click the My Computer icon on your desktop and select **Map Network Drive**, or open Windows Explorer and select **Map Network Drive** from the Tools menu.

2 In the Map Network Drive dialog box, select a drive (or accept the default selection) and type in the SnapServer and directory you want to map using the syntax: \\*server**share*. For example:

\\Snap401178\Share1

3 If you want the drive to be mapped every time you log in, click to put a check in the **Reconnect at logon** box. Click **Finish**.

4 You will be asked for your SnapServer userid and password if it is different than your Windows logon. The drive will then be visible as a network drive.

Connecting a MacOS Client Using SMB

MacOS X clients can connect using SMB as well as AFP.

1 Choose **Go** from the Finder menu bar. In the Connect to Server dialog box, enter one of the following:

```
smb://servername
```

```
smb://ipaddress
```

Click **Connect**.

2 Select a share (called a volume on the Mac) to mount on your desktop.

  a If "guest" is enabled for SMB or if your default log on is a valid SMB user, you will be presented with a share selection dialog box. Choose the share to connect to or click **Authenticate** to log in as a different user. A network icon should appear on your desktop for the share.

  b If a user login prompt displays, enter a username and password. Once authenticated, the share selection dialog box will be displayed. Choose the share to connect to. A network icon should appear on your desktop for the share.

  Note If you configured your Mac not to show drives on the desktop, you can find the SnapServer by selecting **File > New Finder Window** in the menu bar.

3 To access files on the server, double-click the icon for the share. A Finder window will display the contents of the share, and your SnapServer will now behave like any other disk on your Mac.

To disconnect from the SnapServer, drag its icon into the trash.

Windows SMB and security settings are configured from this page. Before performing the configuration procedures provided here, be sure you are familiar with the information provided in Support for Windows Networking (SMB) and Support for Windows Network Authentication.

NFS Access

NFS access to the server is enabled on the **Network > NFS** screen of the Administration Tool. By default, NFS access is enabled and any NFS client can access the SnapServer through the guest account.

Note Only NFS v2 and v3 are enabled by default. If you wish to enable NFS v4, select the **Enable NFS v4** check box on the **Network > NFS** screen.

NFS client access to shares can be specified by navigating to the **Security > Shares** screen and clicking the **NFS Access** link next to the share. If you are in Unicode mode, you must configure the SnapServer's protocol for the code page being used. See "NFS" on page 142 for more information.

Support for NFS

Consider the following technical information when configuring access for your NFS clients.

Supported Protocols

SnapServers support these versions of the NFS protocol:

Protocol	Version	Source
NFS	2.0, 3.0, 4.0*	RFC 1094, RFC 1813, RFC 3530
Mount	1.0, 2.0, 3.0	RFC 1094 Appendix A, RFC 1813, RFC 3530
Lockd	1.0, 4.0	RFC 1094, RFC1813, RFC 3530

* NFS v4 ACLs are not supported.

Supported NFS Clients

SnapServers have been tested with these UNIX-based networking clients:

- Red Hat Enterprise Linux (RHEL) 3.x, 4.x
- Red Hat Fedora 4.x, 5.x, 6.x, 7.x, 8.x, 9.x
- HP-UX 11, AIX 5.3
- Sun Solaris 9, 10
- SuSE Pro 9, 10
- SuSE Linux Enterprise Server (SLES) 8.x, 9.x, 10.x

Note After enabling NFS v4 with Kerberos security, read-write host entries for `gss/krb5`, `gss/krb5i`, and `gss/krb5p` are automatically added to the NFS access entries for each NFS-enabled share.

Apple Networking Configuration

Apple File Protocol (AFP) settings are configured on the **Network > Apple** screen of the Administration Tool. The default settings provide access to AFP clients over an AppleTalk or TCP/IP network. MacOS clients connecting over AFP can log in to the server either as local users on the SnapServer or as Windows NT or Active Directory domain users (if the server belongs to a domain). For more granular control over client access for MacOS users who do not belong to a recognized Windows domain, create local user accounts.

Note MacOS X users can also connect to the SnapServer using Windows networking (SMB). See “Connecting a MacOS Client Using SMB” on page 32.

AFP Configuration Guidelines

Consider the following when configuring access for your AFP clients.

Terminology

Some SnapServer terms may cause confusion for those familiar with Apple terminology.

Term	Definitions
Share	A SnapServer share appears as a Macintosh volume that can be accessed through the Chooser. **Note** Unlike standard AppleShare servers, SnapServers allow nested shares (folders within folders). As a result, it is possible for some files or directories to appear in more than one share.
Volume	A volume on a SnapServer is a logical partition of a RAID's storage space that contains a file system.
Right-click	This document uses the Windows convention in describing keyboard/mouse access to context-sensitive menus. For example, "To rename a group, right-click a group and then choose **Rename**." Macintosh users should substitute control-click to achieve the same result.

Authenticating Clients Against a Configured Windows Domain

You can authenticate AFP clients against a Windows domain by navigating to **Network > Apple** and checking the *Authenticate AFP users against Windows domains* box. When domain authentication is enabled, usernames will first be authenticated against the Windows domain and then authenticated against the local database. Local and domain users with the same name will connect as the domain user. To force either local or domain authentication, prefix the username with the name of the domain to authenticate against or the name of the SnapServer. For example:

`mydomain\username` (domain authentication)

`snap12345\username` (local authentication)

Distinguishing Share Names on the Desktop and Finder

By default, the Chooser identifies SnapServer shares using only the share name. To display both the share name and the server name, the *Add Server Name To Apple Shared Folder Names* check box on the **Network > Apple** screen of the Administration Tool is enabled by default. This option allows Macintosh applications to differentiate between shared folders with the same share name on multiple servers. For example, SHARE1 on SNAP61009 refers to the share named SHARE1 on the SnapServer named SNAP61009.

Supported AFP Clients

The SnapServer supports MacOS 9.x and 10.x clients.

FTP/FTPS Access

FTP and FTPS settings are configured on the **Network > FTP** screen of the Administration Tool. FTPS adds encryption to FTP for increased security. By default, FTP and FTPS clients can access the server using the anonymous user account, which is mapped to the SnapServer's *guest* user account and *AllUsers* group account. You can set share access and file access for anonymous FTP users by modifying permissions for these accounts. For more granular control over FTP access, you must create local user accounts for FTP users.

SnapServer also supports explicit FTPS (i.e., FTPES or Auth TLS).

Note If standard FTP is enabled, only the data channel is encrypted for FTPS connections—the control channel (including user password) is not encrypted. To force FTPS to encrypt the control channel as well, disable standard FTP.

Supported FTP Clients

SnapServers have been tested with the most common FTP clients and work as expected based on the commands required by RFC 959. SnapServers have been proven to work with these products for standard FTP: Internet Explorer 6.0 and later, Safari 2.0 and later, and FireFox 2.0 and later.

Note Most standard FTP clients do not support FTPS. A client designed to support FTPS is required for FTPS connections.

To connect to the server through FTPS:

- Configure your FTPS client application to use explicit FTPS (i.e., FTPES or "Auth TLS").
- Enter the SnapServer's server name or IP address.

HTTP/HTTPS Access

HTTP and HTTPS are used for browser-based access to the server via Web View, Web Root, or the Administration UI. HTTPS enhances security by encrypting communications between client and server, and cannot be disabled. You can, however, disable HTTP access on the **Network > Web** screen of the Administration Tool. Additionally, you can require browser-based clients to authenticate to the server.

Note To access the CA *e*Trust Antivirus configuration interface (on the **Snap Extensions** screen), HTTP must be enabled.

GuardianOS supports the following browers: Microsoft Internet Explorer (6.0 or later), Apple Safari (2.0 or later), and Mozilla FireFox (2.0 or later).

Configuring HTTP/HTTPS

You can require web authentication, disable http (non-secure) access, and enable the Web Root feature.

Using WebRoot to Configure the SnapServer as a Simple Web Server

When you enable the Web Root feature from the **Network > Web** page, you can configure your SnapServer to open automatically to an html page of your choice when a user enters `http://[servername]` or `http://[IP address]` in the browser field.

In addition, files and directories underneath the directory you specify as the Web Root can be accessed by reference relative to `http://[servername]` without having to reference a specific share. For example, if the Web Root points to directory *WebRoot* on share *SHARE1*, the file *SHARE1/WebRoot/photos/slideshow.html* can be accessed from a web browser as `http://[servername]/photos/slideshow.html`.

The Web Root can also be configured to support directory browsing independent of Web View (access through shares).

Note The SnapServer supports direct read-only web access to files. It is not intended for use as an all-purpose Web Server, as it does not support PERL or Java scripting, animations, streaming video, or anything that would require a special application or service running on the server.

Accessing the Admin Tool when Web Root is Enabled

By default, when you connect to a SnapServer with web root enabled, the browser will load the user-defined HTML page or present a directory listing of the Web Root. To access the Administation Tool (e.g., to perform administrative functions, change a password, etc.), enter the following in the browser address field:

```
http://[servername or ip address]/config
```

You will be prompted for your User ID and password, then you will be placed into the GuardianOS UI.

If you need to access the Web View page to browse shares on the server independent of Web Root, enter this in the browser address:

```
http://[servername or ip address]/sadmin/GetWebHome.event
```

Web View

Web View opens when the user accesses a SnapServer using a Web browser, unless the administrator has enabled the Web Root feature (see “Using WebRoot to Configure the SnapServer as a Simple Web Server” on page 37). This screen displays a list of all shares to which the user has access. Users can navigate the share structure to locate and view or download files, but they cannot modify or upload files.

For users with admin rights, a key icon 🔑 appears next to the file/folder in the share. Clicking this icon displays a popup box with security information about the file/folder.

From this screen, the user can also change a password, switch to another user, or log in to perform Administrative functions (if the user has Administrator permissions).

To Switch to a Different User

Users can switch to a different username from the opening Web View screen by clicking the **Switch Users** link and entering the new username and password.

To Change a User Password

Users can change their passwords from the opening Web View screen by clicking the **Change Password** link, and then completing the username, old password, and new password information.

DHCP Server

DHCP server settings are configured on the **Network > DHCP** screen of the Administration Tool. To configure the SnapServer as a DHCP server, it must have a static IP address. The DHCP server automatically uses the subnet of the IP address you set up.

Ensure that the network has no other active DHCP servers. You may negatively impact the network if you enable the SnapServer as a DHCP server while another server on the network is performing this function.

When you enable the SnapServer as a DHCP server, it reports in-use IP addresses at the bottom of the screen under Current DHCP Status.

Print Server

The SnapServer can be configured to emulate a Windows print server for locally-attached USB printers. Client machines connect to the SnapServer over the network and use the printer similarly to using a printer shared by a Windows or CUPS server. You can pause or resume the printer, and monitor or cancel print jobs using the Administration Tool.

Configuring your SnapServer as a print server is a two part process:

- Configure the printer on the SnapServer.
- Configure the client to print via the SnapServer.

Configuring the Printer on the SnapServer

1. Connect the printer to one of the USB ports on the SnapServer.
2. Power on the printer.
3. In the SnapServer's Administration Tool, navigate to **Server > Printing**. A list of currently defined USB printers is displayed. To add the new printer, click **Add Local Printer**.
4. The SnapServer will detect the new printer and it should appear as an option in the **Local Printer Device** dropdown list. Select that printer.
5. Give the printer a name, and complete Desciption and Location information as desired. Click **OK**. The printer will appear in the list on the main printing page.

Adding the Network Printer to the Client

The SnapServer supports both Windows SMB and IPP printing protocols.

Note To make printer drivers easily accessible to users, copy them to a share that everyone can access on the SnapServer. The SnapServer cannot be configured to automatically provide printer drivers to clients.

Adding the Network Printer to a Windows Client

Windows offers several methods for adding a printer. Follow your usual printer configuration method to add a printer shared on a SnapServer. When asked to locate the printer:

- To use SMB, enter the SnapServer name or IP address, or browse to the server to choose the printer share.
- To use IPP, enter the exact path as follows in the URL field:

  `http://`*`servername`*`:631/printers/`*`sharename`*

  where *servername* is the name or IP address of your SnapServer and *sharename* is the name of the printer.

  Note 631 is the IPP port number.

If you experience difficulty adding the printer, try the following:

1. Navigate to **Start > Run** and enter the server name as follows: \\servername
2. After a delay, you may be prompted for a user name and password. Log in as a user with access to the SnapServer.
3. A Windows Explorer window will open displaying all shares and printers on the server. Right-click the server and choose **Connect**.
4. Follow the instructions to provide the printer driver and complete the set up.

Adding the Network Printer to a Mac OS X Client

Add a printer using your usual method. If you are using SMB, you will need to know the SnapServer name. If you are using IPP, you will need to enter the IP address in the **Type** field and the printer and sharename in the **Queue** field.

Adding the Network Printer to a Linux Client

Add a printer using your usual method. If you are using SMB, you will need to know the SnapServer name. If you are using IPP, enter the exact path as follows in the URL field:

`http://servername:631/printers/sharename`

where *servername* is the name or IP address of your SnapServer and *sharename* is the name of the printer.

Note 631 is the IPP port number.

Monitoring Print Jobs Using the Administration Tool

Pause or resume the printer, and check the status of or cancel print jobs from the SnapServer's Administration Tool.

To Pause the Printer

1. Navigate to **Server > Printing** and click the Status link next to your printer to open the Job Status window and see your print job queue.
2. Click the **Pause Printer** button to pause all print jobs.

Note When the printer is paused, the button will become a **Resume Printer** button, which you can click to resume printing.

To Cancel or Check the Status of Print Jobs

1. Navigate to **Server > Printing** and click the Status link next to your printer to open the Job Status window and see your print job queue.
2. To cancel a print job, click to put a check in the box next to the job you want to remove and click **Cancel Selected Jobs**. You can select to cancel multiple jobs. If you want to cancel all the listed print jobs, click the **Cancel All Jobs** button. Click the **Refresh** button to update the screen with the current list of print jobs.

Deleting a Printer from the SnapServer

When you remove a printer, remember to remove its information from both the Administration Tool and the client machines.

1. Disconnect the printer cable from the SnapServer.
2. In the Administration Tool, navigate to **Server > Printing**. In the list of printers, the status of printer you just removed should appear as Offline.
3. Click the printer link to open the Edit Printer page, then click the **Delete** button to delete the printer.

User & Group Management

Authentication validates a user's identity by requiring the user to provide a registered login name and corresponding password. SnapServers ship with predefined local users and groups that allow administrative and guest user access to the server via all protocols. Administrators may choose to join the SnapServer to a traditional Windows NT or Active Directory domain, and Windows clients can then authenticate to the server using their domain credentials. To accommodate NFS clients, the SnapServer can also join an NIS domain, and the SnapServer can look up user and group IDs maintained by the domain. For authentication control beyond the guest account, Macintosh and FTP client login credentials can be created locally on the sever.

Topics in User and Group Configuration:

- Default User and Group Settings
- UID and GID Assignments
- Local Users and Groups
- NIS Domain

Default User and Group Settings

SnapServer default security configuration provides one share to the entire volume. All network protocols for the share are enabled, and all users are granted read-write permission to the share via the guest account.

A *local user* or *group* is one defined locally on a SnapServer using the Administration Tool. The default users and groups listed below cannot be modified or deleted.

Default Local Users and Groups	
admin	The admin user account is used to log into the Administration Tool. The default password for the admin account is also *admin*.
guest	The guest user account requires no password.
AllLocalUsers	The AllLocalUsers group account includes all local users created on the SnapServer.
AllUsers	The AllUsers group account includes all local, Windows domain, and NIS users.
admingrp	The Admin group account includes the default admin user account. Any local user accounts created with admin rights are also automatically added to this group.

Domain	
Windows	The SnapServer can join a Windows NT domain or an Active Directory domain.
NIS	The SnapServer can join an NIS domain and function as an NIS client.

UID and GID Assignments

The SnapServer uses the POSIX standard to assign a user ID (UID) and group ID (GID), in which each user and group must have an ID. This requirement applies to all users and groups on the SnapServer, including local, Windows, and NIS users and groups.

If you join the SnapServer to a Windows or NIS domain, IDs are automatically assigned. UIDs and GIDs are now assigned on a “first come, first served” basis, with preference given first to local users, then Windows users, then NIS users.

Consider the following when creating users and groups:

- UIDs and GIDs from 0 - 100 are unavailable for use. If you try to assign a UID or GID that is in use by NIS or the Windows domain, or is less than 101, you will get an error message.

- When the server automatically generates UIDs or GIDs for imported Windows domain users or groups, UIDs or GIDs that are already in use by local and NIS users will be skipped.
- When NIS domain users and groups are imported, the SnapServer will discard any that are less than 101 or are in conflict with UIDs already in use by local or Windows domain users and groups.

The NIS user ID ‘nobody’ (UID 65534) is reserved. It is not mappable to another ID, nor is another ID mappable to ‘nobody’.

GuardianOS offers ID Mapping, which allows mapping of Windows users to local or NIS users to provide unified permission assignments to users of different protocols. For more information on ID Mapping, please see “ID Mapping” on page 102.

Local Users and Groups

Local users or groups are created using the **Security > Local Users** and **Security > Local Groups** screens in the Administration Tool. Local users and groups are used for administrative and guest access to the server. Windows Workgroup, Macintosh, and FTP clients initially access the server using the guest account. If you require a higher degree of control over individual access to the file system for these clients, you must create local accounts (or, in the case of Windows, use Windows NT domain or Active Directory security).

Guidelines for Local Authentication

Duplicating Client Login Credentials for Local Users and Groups

To simplify user access for Windows Workgroup or Macintosh clients, duplicate their login credentials on the SnapServer. That is, create local accounts on the SnapServer that match those used to log into client workstations. This strategy allows users to bypass the login procedure when accessing the SnapServer.

Caution This strategy applies only to local users. Do not use duplicate domain user login credentials.

Default Local Users and Groups

The default local users and groups (see “Default User and Group Settings” on page 44) cannot be modified or deleted. Default users and groups *admin*, *guest*, and *admingrp* appear on the list of users or groups on the User or Group Management screens, but they cannot be deleted or modified. As you would expect, the default local users and groups do appear on the Share Access and Quotas screens.

Changing Local UIDs or GIDs

The SnapServer automatically assigns and manages UIDs and GIDs. Because you may need to assign a specific ID to a local user or group in order to match your existing UID/GID assignments, the SnapServer makes these fields editable.

Password Policies

To provide additional authentication security, set password character requirements, password expiration dates, and lockout rules for local users.

Local users can also be individually exempted from password expiration and character requirement policies. The built-in *admin* user is exempt from all password policies.

Note Local users with expired passwords can change their passwords at http://<snapservername>/changepassword.

Local Account Management Tools

The SnapServer offers the following tools for creating, modifying, and editing local user and group accounts.

Function	Navigation Path
Local User Management	Navigate to the **Security > Local Users** screen, from which you can create, view, edit, and delete local users. You can also set user password policy, including password character requirements, maximum number of allowed logon failures, and password expiration settings.
Local Group Management	Navigate to the **Security > Local Groups** screen, from which you can create, view, edit, and delete local groups.

Notes

- Local users can be individually exempted from password expiration and character requirements. This may be necessary for some special users, such as users configured to perform backups. See the Online Help for procedures to set password policy for local users.
- The built-in *admin* user is automatically exempt from all password policies.

Note Changing a user’s UID will nullify any file system access permissions that apply to that UID. In addition, any existing permissions for a UID previously assigned to a user changed to a different UID will become active if another user is created with the same UID. Carefully consider security configuration on existing files and directories before changing the UID of a user.

NIS Domain

NIS domains are configured on the **Network > NIS** screen of the Administration Tool. The SnapServer can join an NIS domain and function as an NIS client. It can then read the users and groups maintained by the NIS domain. Thus, you must use the NIS server to make modifications. Changes you make on the NIS server do not immediately appear on the SnapServer; it may take up to 10 minutes for changes to be replicated.

Guidelines for Configuring NIS

Handling UID/GID Assignments

Unless UID/GID assignments are properly handled, NIS users and groups may fail to display properly. For guidelines on integrating compatible SnapServer UIDs, see “UID and GID Assignments” on page 44.

NIS identifies users by UID, not user name, and although it is possible to have duplicate user names, Overland Storage does not support this configuration.

Storage Configuration and Expansion

Note Much of the configuration discussion presented here is not applicable to SnapServers with fewer than four (4) drives. For SnapServer 110 and 210, see the *User's Guide for SnapServer 110 and 210* for storage configuration guidelines.

SnapServers with four to eight drives are preconfigured as a single RAID 5, SnapServers with twelve drives are preconfigured with a single RAID 6, and SnapServer 110 and 210 are preconfigured with a single RAID 0. Each server's disk space is preconfigured with a single volume encompassing 80 percent of available capacity and a single share pointing to the volume. The default storage configuration reserves 20 percent of the data space for snapshots (including servers that require a license to activate snapshots). If the default configuration is appropriate for your needs, you need only create the directory structure, set share access permissions, and (optionally) schedule snapshots.

You may have requirements that demand a different configuration. For example, if the information on a SnapServer is mission-critical but infrequently accessed, creating a RAID 1 may be a more suitable configuration. In another example, some administrators prefer to keep certain sensitive data, such as financial records, in a separate file system for added security.

Topics in Storage Configuration:

- Default Storage Configuration
- Changing the Default Storage Configuration
- RAIDs
- Volumes
- Quotas
- Data Migration
- Expansion Arrays
- Disks and Units

Default Storage Configuration

The default storage configuration for all SnapServer and exapnsion models is shown in the table below. Each server's disk space has a single volume, and a single share pointing to the volume. The share access settings of the default share grant access to all users and groups over all protocols. The data space is preconfigured to allocate 80 percent of the RAID for the file system and the remaining 20 percent for snapshots.

Drives / RAID	SnapServer 110	1-disk RAID 0
	SnapServer 210	2-disk RAID 0
	SnapServer 410 SnapServer 520 SnapServer 550 SnapServer 620 SnapServer 650	4-disk RAID 5 (No hot spare configured)
	SnapServer N2000	4-disk RAID 5 12-disk RAID 6
	SnapServer E2000 Snap Expansion S50	up to 12-disk JBOD

Allocation	Volume	80% of RAID capacity is allocated to the default volume.
	Snapshot Pool	20% of RAID capacity is allocated to the snapshot pool.

Security	Shares	A single share points to the volume.
	Share Access	Grants read/write access to all users and groups over all protocols.
	Security Model	Windows-style file-level security (can be changed to UNIX)

Changing the Default Storage Configuration

The SnapServer's flexible storage architecture allows for a wide variety of implementations to suit many different storage needs. In some cases, administrators may change the default configuration to increase capacity by modifying the configuration of the SnapServer, or attaching one or more expansion arrays.

When a backup scheme does not require backing up from a snapshot, or when a backup window can be used while files are not active, the snapshot space can be reclaimed for storage on the data volume. In cases when backup is ongoing or very frequent, a RAID 0 configuration may be most appropriate. In cases where multiple expansion arrays are attached to the SnapServer, a combination of a RAID 1 and hot spares may be the optimal configuration for the SnapServer. See the online help for more information.

RAIDs

RAIDs are created, viewed, edited, and deleted from the **Storage > RAID Sets** screen of the Administration Tool. SnapServers with four to eight drives ship with all disk drives configured as a RAID 5. SnapServers with twelve drives ship with all disk drives configured as a RAID 6. SnapServers with one or two drives ship with the drive(s) configured as a RAID 0. Before changing the default RAID configuration, consider the following information on the SnapServer's RAID implementation.

Note Much of the configuration discussion presented here is not applicable to SnapServers with fewer than four (4) drives. For SnapServer 110 and 210, see the *User's Guide for SnapServer 110 and 210* for storage configuration guidelines.

Factors in Choosing a RAID Type

The type of RAID configuration you choose depends on a number of factors:

- The importance of the data
- Performance requirements
- Drive utilization
- The number of available drives

For example, in configuring the disk drives of a four-drive SnapServer, the decision whether to include a hot spare in the RAID depends on the value you place on capacity vs. high availability. If capacity is paramount, you would use all drives for storage; if high availability were more important, you would configure one of the drives as a hot spare. The following table summarizes the advantages and disadvantages of each type of RAID.

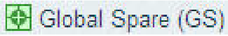
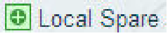
Features	RAID 0	RAID 1	RAID 5	RAID 6	RAID 10
Data Loss Risk	Highest	Lowest	Low	Lower	Very Low
Write Access Speeds	Fastest	Fast	Medium	Slower	Faster
Usable Capacity	Highest	Lowest	High	Medium	Low
Disks Required	1 or more	2 or more	3 or more	4 or more	4 or more
Supports Hot Spares	No	Yes	Yes	Yes	Yes

Caution To reduce exposure to double-drive disk failures on RAID 5, use no more than eight drives in a single RAID set and group smaller RAID sets together.

Local and Global Hot Spares

A *hot spare* is a disk drive that can automatically replace a damaged drive in a RAID 1, 5, 6, or 10. Designating a disk drive as a hot spare helps ensure that data is available at all times. If one disk drive in a RAID fails or is not operating properly, the RAID automatically uses the hot spare to rebuild itself without administrator intervention. SnapServers offer two kinds of hot spares: local and global.

Item	Description
Definitions	**Local (hot) spare** — A local (or dedicated) hot spare is associated with and is available only to a single RAID. Administrators typically create a local hot spare for RAIDs containing mission-critical data that must always be available. **Global (hot) spare** — A hot spare that may be used for any RAID 1, 5, 6, or 10 in the system (assuming sufficient capacity) as necessary.

Item	Description
Identifying	Hot spares are identified on the **Storage > Disks/Units** screen using the following icons:  Global Spare (GS)  Local Spare Each icon will be associated with a disk in the RAID, identifying that disk as either a local hot spare or a global hot spare.
Interaction	When a drive in a RAID fails, the system looks for a hot spare in the following order: 1 If a local hot spare dedicated to the RAID exists, use the local hot spare. 2 If no local hot spare is available, and there is a single hot spare of sufficient capacity, use the global hot spare. 3 If no local hot spare is available, and two global hot spares of different capacity are available, use the smaller hot spare with sufficient capacity.

Automatic Incorporation of Hot-Swapped Drives

If a RAID (except RAID 0) is running in degraded mode and a raw drive, a non-GuardianOS drive, or an unassigned GuardianOS-partitioned drive is "hot-inserted" into a SnapServer, it can be automatically assigned as a local spare and used to rebuild the degraded RAID. If there are no degraded RAIDs, a hot-inserted non-GuardianOS or unassigned drive will be automatically configured as a global hot spare. To enable the automatic incorporation of an unassigned drive, go to the **Storage > RAID Sets** screen and click the **RAID Settings** button.

Background Disk Scan

The background disk scan checks the integrity of RAID data by continuously scanning the disk drives for errors. Each RAID (except RAID 0) has its own background disk scan that is set to run when the I/O activity falls to a very low disk activity. Once the activity rises above the *idle threshold*, the background scan stops and waits for the activity to fall to the idle threshold again before resuming. As a result, there should be minimal to no impact on performance. Once the disk scan has completed a pass on a given RAID set, it waits a certain period of time before starting again.

The background disk scan is enabled by default. To disable the background disk scan, go to the **Storage > RAID Sets** screen and click the **RAID Settings** button.

Notes

- If the background disk scan is disabled, it will still initiate a scan on a RAID if problems are detected on one of the RAID drives.
- The background scan will not run on RAIDs that are degraded, syncing, or rebuilding.

RAID Management Tools

SnapServers use the following tools for configuring and monitoring RAIDs:

Function	Navigation Path
Ongoing Maintenance	Navigate to the **Storage > RAID Sets** screen, from which you can create, assess, edit, and delete RAIDs. You can also disable or enable the Background Disk Scan and the automatic assignment of GuardianOS-partitioned unused disks to a degraded RAID.
Email Notification	The server can notify you when a RAID is degraded, failed, or has experienced another error or maintenance condition. This allows you to take action to ensure workflows are not disrupted (**Server > Email Notification**).

You can view the status of your RAID sets on the **Storage > RAID Sets** and **Monitor > System Status** screens.

RAID Groups

Two RAIDs can be grouped together to neatly resolve a number of capacity issues. For example, a volume on one RAID nearing full utilization can be expanded using spare capacity on another RAID. The ability to grow volumes beyond the capacity of a single RAID allows administrators to expand a volume without reconfiguring RAIDs and allows users to continue working as usual with no interruption.

Grouped RAIDs must be the same type; you can group two RAID 1s or two RAID 5s (e.g., you cannot group a RAID 1 and a RAID 5).

Note Only RAIDS of the same PE (physical extent) size can be grouped. If you are growing the volume on one RAID to use free capacity on another RAID, you will only be allowed to select from those RAIDs that can be grouped.

Also consider the following:

Adding an Expansion Array

In a common scenario, a four-drive SnapServer configured as a RAID 5 is nearing full utilization. The administrator decides to add an expansion array. The administrator creates a RAID 5 on the expansion array, groups it with the existing RAID on the SnapServer, and then expands the size of the original volumes using the new storage from the expansion array.

Grouping RAIDs with other Grouped RAIDs

Just as RAIDs can be grouped, individual groups of RAIDs can be brought together to form an even larger group. For example: A 1 TB SnapServer is running out of capacity. Two 1 TB 12-drive expansion arrays are attached to the SnapServer to provide increased capacity. You can configure a RAID 5 on each of the expansion arrays, then group them together. The resulting RAID group can then be grouped with the RAID on the SnapServer, allowing network users to take advantage of the full capacity of the head and expansion arrays with no loss of capacity.

Deleting Grouped RAIDs

Deleting the RAID Group will delete all member RAIDs, all their volumes and shares, and all their data. If one RAID becomes inaccessible for any reason, the entire RAID group will also become inaccessible. Depending on the cause, the RAID group may or may not be recoverable. For example, if a RAID group spans a host SnapServer and an expansion array and one of the RAIDs goes down because of a disconnected cable, the RAID group is fully recoverable by reconnecting the cable and rebooting the system. On the other hand, if one of the RAIDs becomes corrupted and remains unrecoverable, the data in the other RAID will also be lost.

Snapshot Pools are Combined

When two RAIDs are grouped, the size of the resulting snapshot pool is the sum of each RAID’s formerly separate snapshot pools.

Two RAIDs at a Time

To group more than two RAIDs, create a RAID group with two RAIDs, then group the RAID group with each RAID one at a time.

You can view your RAID group status from either the **Storage > RAID Sets** or **Monitor > System Status** screen.

Note Only RAIDs of the same PE size can be grouped. The Web UI will notify you if you attempt to group two RAIDs with different PE sizes.

Volumes

Volumes are created, viewed, edited, and deleted from the **Storage > Volumes** screen of the Administration Tool. The default volume organizes the SnapServer's storage capacity into a single volume with a single file system. If you need separate file systems on the same server, you can delete the default volume and create two or more smaller volumes in its place. Consider the following facts and guidelines when planning your new volume configuration.

Volumes and the Snapshot Pool

The default disk and RAID capacity is divided between the file system (80 percent) and the space left available for future snapshot use (20 percent). You may need to adjust this figure depending on your snapshot strategy or expand the volume to all available space if you plan never to use snapshots. Keep in mind that you can increase or decrease snapshot pool size at any time, but volume space can only be increased. For more information, see "Estimating Snapshot Pool Requirements" on page 113.

Note GuardianOS snapshots should not be used on volumes that contain iSCSI disks. If a volume will contain one or more iSCSI disks, decrease the Snapshot pool size to zero. For information about creating snapshots of iSCSI disks, see "Configuring VSS/VDS for iSCSI Disks" on page 93.

Deleting Volumes

Deleting volumes may move or disable certain third party applications that are installed on the user volume space.

The NetVault for GuardianOS Database Directory (NVDB), containing files that keep track of the data you back up; the antivirus software; and Snap EDR reside on the default volume. If you delete the default volume, these components will also be deleted unless there is available space on additional volumes (e.g., on expansion arrays).

To retain NVDB information, you must back up the NVDB directory (see page 120) before you delete the volume, create your new storage configuration, and then restore the directory.

After creating your new storage configuration, you can reinstall the antivirus software by navigating to the **Snap Extensions** screen and selecting **CA Antivirus**. On the next screen, check the **Enable** check box and click **OK**. The SnapServer reinstalls the antivirus software (using default settings) on the volume with the most available space. However, the installation process does not preserve custom antivirus configuration settings, so make a note of any such settings before deleting a RAID or the volume. To reconfigure the antivirus software, click **Configure eTrust Antivirus**.

To reactivate Snap EDR functionality after creating a new volume, download the Snap EDR package from the SnapServer web site and install it on the server using the OS Update feature. Then click the **Snap EDR** link in the Site Map (under Extras) and click the **Start** button.

Note If the volume on which the NVDB directory, antivirus software, or Snap EDR resides is deleted, the system attempts to move the items to another volume with the most available space. If no other volumes are available, the items are automatically disabled.

Note If you delete a volume, you will also delete any iSCSI disks that reside on that volume.

Expanding Volume Capacity

A volume's capacity can be expanded by navigating to the **Storage > Volumes** screen and clicking the name of a volume. There are two ways to expand the size of a volume:

- **Adding Unallocated Capacity —** If there is unallocated capacity remaining on the RAID, you can add this capacity to the volume by editing the Volume size field or clicking the **Grow to Max. Size** button, and then clicking **OK**.
- **Creating a New RAID —** If all capacity on the RAID is allocated, and either: (1) a sufficient number of drives to create a new RAID exists, or (2) a RAID of the same type with excess capacity exists, the **Expand Volume** button appears. Click this button to create an additional RAID, group the RAID with the existing RAID, and expand the volume into the space on the new RAID.

  Note If you expand the volume onto an existing RAID with existing volumes, those volumes will be preserved and the expanded volume will only consume the free space on the RAID.

A volume can be expanded up to 16 TBs, either as a standalone volume or as a volume group.

Security Models, SnapTrees, and Volumes

Volumes are created with the Windows security model (which can be changed in the **Securities > SnapTrees** page or when creating a share to point to the volume root). Directories created in the root of a volume (aka SnapTree directories) in the Web UI are automatically assigned either a Windows- or a UNIX-style security model, based on the security model of the parent volume (this can also be subsequently changed in the SnapTrees page or when creating a share pointing to them). The security model determines the file-level security scheme that will apply to files and folders within the volume or SnapTree directory.

Configuring Write Cache

Note Not related to write cache on iSCSI disks. For information about configuring write cache on iSCSI disks, see "Write-Cache Options with iSCSI Disks" on page 89.

By default, write cache is enabled on all volumes. For systems that do not use a UPS device to help protect data during a power outage or for applications that require synchronous writes to disk, write cache can be disabled on a volume by volume basis. When a volume's write cache is disabled, all data written to the volume bypasses memory buffers and writes directly to disk, helping to protect the data when writes are occur during a power outage. While disabling write cache does help protect data, it also significantly impacts disk write performance. For the procedures to disable write cache on new and existing volumes, see To Disable/ Enable Write Cache on a New Volume or To Disable/Enable Write Cache on an Existing Volume.

Note When write cache is disabled on a volume, disk cache is also disabled on all disk drives that are members of the RAID or RAID group hosting the volume. This can impact performance on other volumes with write cache enabled that are hosted by the same RAID or RAID group.

Note Not all disk drives support disabling write cache. If any of the volume's drives are IDE drives, you will not have the option to disable write cache for that volume. In addition, write cache can not be disabled on SnapServer 18000 or the SD30 expansion unit.

Checking Filesystems

Filesystems on individual volumes can be checked for errors and repaired, if necessary. The root volume can also be checked, and any errors found will automatically be repaired. Since the GuardianOS automatically checks the root volume for errors if any of a number of triggers occurs (e.g., a power outage, failure of the volume to mount, etc.), it is recommended that the root filesystem check feature only be used when directed by a Technical Support representative. See the Volumes section in the Online Help for procedures to check the volume filesystems.

Volume Management Tools

The SnapServer offers several tools for monitoring and controlling how storage space on a volume is used.

Function	Navigation Path
Ongoing Maintenance	Navigate to the **Storage > Volumes** screen, from which you can create, view, edit, and delete volumes.
Email Notification	The server can notify you when a volume is full. This allows you to increase volume size or take other actions to ensure workflows are not disrupted (**Server > Email Notification**).
Volume Usage	You can view the current utilization totals for each volume, from the **Storage > Volumes** screen.
Quotas	Use quotas (**Storage > Quotas**) to limit the amount of storage space on a volume that specific users or groups can consume. See Quotas for more information.

You can view volume status from the **Storage > Volumes** screen.

To Check the Root Filesystem

Caution Checking the root filesystem requires a reboot of the server.

1. Select the **Check Root Filesystem** link.
2. On the page that opens, click the **Check Filesystem** button.
3. Click **Yes** when informed that a reboot will be required.
4. To view a log of the results, click the **View Log** button.

To Check a Filesystem on a Volume

Click the **Check Filesystem** link to check and repair the filesystem on this volume. You can configure GuardianOS to run this check on three levels:

- **Do not repair errors** — This option will check for errors, but will not repair them. It is recommended that you do this periodically, especially following a power outage or any other unconventional outage.
- **Repair errors** — It is recommended that you run this level if you suspect file system damage may have occurred (e.g., if a previous **Do not repair errors** operation reported file system errors).
- **Repair errors (aggressive)** — It is only recommended that you run this level if you have been advised to do so by SnapServer Technical Support, or if **Repair errors** has failed to solve the problem and you are willing to risk loss of data.

To start the filesystem check, select the level and click **Check Filesystem**. The progress of the filesystem check will be displayed while it runs.

You can view a log of the filesystem check by clicking **View Log**.

Quotas

Quotas are configured in the **Storage > Quotas** screen of the Administration Tool. Assigning quotas ensures that no one user or group consumes a disproportionate amount of volume capacity. Quotas also keep tabs on how much space each user (or NIS group) is currently consuming on the volume, allowing for precise tracking of usage patterns. You can set individual quotas for any local, Windows domain, or NIS user known to the SnapServer. Group quotas are available only for NIS groups.

Default Quota Assignments

For users and groups, there are no pre-assigned default quotas on the SnapServer. When quotas are enabled on the SnapServer, you can assign a default quota for all users, or allow all users to have unlimited space on the volume.

Unless you assign individual user or group quotas, all users and groups will receive the default quota.

How the SnapServer Calculates Usage

In calculating usage, the SnapServer looks at all the files on the server that are owned by a particular user and adds up the file sizes. Every file is owned by the user who created the file and by the primary group to which the user belongs. When a file is copied to the server, its size is applied against both the applicable user and group quota (NIS groups only).

Setting User Quotas

You can set individual quotas on a per-volume basis for any local user, Windows domain user, or NIS user or group known to the SnapServer.

Note Specific individual user quotas always override the default quota.

Data Migration

Use the Data Migration feature to migrate data from a legacy SnapServer or other computer that supports CIFS or NFS (v2 or v3) to a new SnapServer. The Data Migration (DM) feature can be used to copy or move files and folders from a server on the network (source) to a SnapServer (target).

To access the Data Migration utility, navigate to **Maintenance > Data Migration**.

If an error is encountered during migration (e.g., a file or folder is locked and cannot be migrated), the DM utility records the error in a log, and continues the operation. When the migration is completed, the administrator can view the log of migration errors. Once the errors have been corrected, the user returns to the DM main screen, and recreates the migration. With the exception of the password, all fields will still be populated with the specifications of the last job.

The following migration options can be specified:

- Copy or move data
- Include subfolders
- Overwrite existing files
- Preserve the original permissions settings

  Note If you elect to preserve original permissions settings, be sure to review Preserving Permissions.
- Verify migrated data

  Note If you elect to verify migrated data, all data will be read twice, once for migration and once for comparison to the copied data. This could be a lengthy process.

For details about setting up a migration job, see the online help.

Note If a migration failed, it is strongly recommended that you enable the **Verify migrated data** option for the re-migration.

Preserving Permissions

The types of permissions retained will differ, depending on which of the following migration scenarios is applied:

Migrating from a Windows Security Model to a Windows SnapTree

If you are migrating from a Windows server (or other type of server that follows the Windows security model) to a Windows SnapTree on a SnapServer, permissions will be retained exactly as they exist on the source. However, as is the case when moving files with permissions between Windows servers, permissions for users that are unknown on the target server will be retained but not enforced. This includes permissions for:

- Local users on the source machine.
- Domain users for domains unknown to the SnapServer (e.g., trusted domains, if the SnapServer is not configured to support trusted domains).
- Certain built-in Windows users and groups.

Migrating from a UNIX Security Model to a UNIX SnapTree

If you are migrating from a UNIX server to a UNIX SnapTree, UNIX permissions for UIDs/GIDs are copied exactly from source to target; thus, identities of the users and groups will be best retained if the SnapServer belongs to the same NIS domain as the UNIX server.

Migrating Between Conflicting Security Models

When migrating from a Unix source to a Windows SnapTree, Unix permissions will be retained and the security personality on the resulting files and directories will be Unix.

However, when migrating from a Windows source to a Unix SnapTree, permissions cannot be retained (since Unix snaptrees are required to be Unix personality throughout). Files and directories will inherit the Unix personality and will have a set of default Unix permissions.

Migrating from a GuardianOS Server

When migrating from one GuardianOS server to another, it is recommended that you maintain the same security model on the target server that you have on the source.

- If your source server uses a Windows SnapTree and has permissions assigned to Windows domain users, use a Windows connection for migration. Windows permissions will be retained exactly as they are on the source, with the same enforcement limitations for unknown users as for migration from Windows servers (see Migrating from a Windows Security Model to a Windows SnapTree).

  Note If migrating from a pre-5.0 GuardianOS server, Windows permissions will be retained verbatim, but may have different meaning due to the differences between the pre-5.0 POSIX ACL security model and the Windows security model introduced in 5.0.

- If your source server uses a UNIX SnapTree and has permissions assigned to local or NIS users, use an NFS connection for migration.

  Note Local users that have UNIX permissions on the source will not be created on the target with the same UIDs.

Migrating from a SnapOS Server

When migrating from a SnapOS Server to a GuardianOS server, permissions will not be correctly retained.

Expansion Arrays

Note This section only applies to SnapServer models that can attach an expansion array. See the *Configuration and Hardware Options Guide* for expansion array options.

Note If GuardianOS detects an expansion unit that is not integrated with the SnapServer, a warning displays across the top of the Disks/Units screen with a link to information about the orphan expansion unit.

To increase the capacity of a SnapServer, Overland Storage offers the SnapServer EXP E2000 and the Snap Expansion S50 expansion arrays. Details on installing a SnapServer E2000 or a Snap Expansion S50 are provided in the *Quick Start Guide* that comes packaged with the array. The guide is also available for download from http://www.snapserver.com/support.

SnapServer EXP E2000

The SnapServer EXP E2000 is a 2U expansion array with up to twelve SATA II or SAS disk drives, or a combination of SAS and SATA disk drives up to a maximum of 12. It ships as a set of unassigned disks with no RAID configuration. Up to five SnapServer E2000s can be connected to a SnapServer NAS N2000.

Note Specific configurations are recommended when SAS and SATA drives (or drives with different rotational speeds) are combined in the same expansion array. Be sure to review “Adding New Disk Drives to Increase Capacity” on page 68 before configuring a mixed-drive array.

A SnapServer E2000 expansion array is accessed and managed through the SnapServer to which it is connected. The expansion array has no physical connection to the network. After the SnapServer E2000 is installed and powered on (see the *E2000 Quick Start Guide* for details), the array’s disk drives appear as unassigned drives, allowing the administrator to configure RAIDs as necessary.

Snap Expansion S50

The Snap Expansion S50 storage subsystem is a 2U expansion array with up to twelve SAS or SATA II disk drives, or a combination of SAS and SATA disk drives up to a maximum of 12. It ships as a set of unassigned disks with no RAID configuration. Up to seven Snap Expansion S50s can be connected to a SnapServer 520, 550, 620, 650, or 18000. Up to three Snap Expansion S50s can be connected to a SnapServer 4500.

Note Specific configurations are recommended when SAS and SATA drives (or drives of different rotational speeds) are combined in the same expansion array. Be sure to review "Adding New Disk Drives to Increase Capacity" on page 68 before configuring a mixed-drive array.

A Snap Expansion S50 expansion array is accessed and managed through the SnapServer to which it is connected. The expansion array has no physical connection to the network. After the S50 is installed and powered on (see the Quick Start Guide for details), the array's disk drives appear as unassigned drives, allowing the administrator to configure RAIDs as necessary.

Preparing the SnapServer

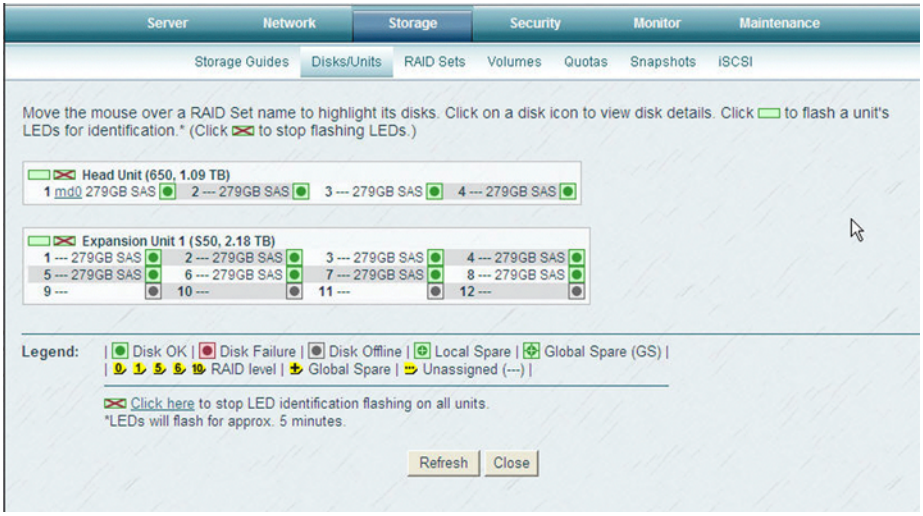
Some SnapServers ship with an HBA installed for connectivity to one or more expansion arrays. If your server already has an expansion HBA, no further preparation (other than preparing rack space) is necessary. To connect an expansion array to a SnapServer that does not have an expansion HBA, you will need to purchase and install the HBA, available from an authorized SnapServer reseller.

Note If you plan to add an expansion HBA to a SnapServer 4500, make sure there is an available PCI slot.

Managing Expansion Array Storage

Disk drives on expansion arrays are not preconfigured, but are shipped as unassigned disk drives, allowing administrators to configure the array as appropriate.

The **Storage > Disks/Units** screen displays the head unit and any expansion arrays attached to the head unit. For more information about the Disk/Units screen, please see “Disks and Units” on page 67.



Move the mouse over a RAID Set name to highlight its disks. Click on a disk icon to view disk details. Click ▭ to flash a unit's LEDs for identification.* (Click ☒ to stop flashing LEDs.)

▭ ☒ Head Unit (650, 1.09 TB)
1 md0 279GB SAS ● 2 --- 279GB SAS ● 3 --- 279GB SAS ● 4 --- 279GB SAS ●

▭ ☒ Expansion Unit 1 (S50, 2.18 TB)
1 --- 279GB SAS ● 2 --- 279GB SAS ● 3 --- 279GB SAS ● 4 --- 279GB SAS ●
5 --- 279GB SAS ● 6 --- 279GB SAS ● 7 --- 279GB SAS ● 8 --- 279GB SAS ●
9 --- ● 10 --- ● 11 --- ● 12 --- ●

Legend: | 🟩 Disk OK | 🟥 Disk Failure | ▨ Disk Offline | ⊕ Local Spare | ⊕ Global Spare (GS) |
| 0 1 5 6 10 RAID level | + Global Spare | --- Unassigned (---) |

☒ Click here to stop LED identification flashing on all units.
*LEDs will flash for approx. 5 minutes.

The disk drives of an expansion array are completely integrated into the host SnapServer’s logic. The default RAID configurations can be deleted and the internal and external disk drives recombined as necessary. For example, to create one large RAID, you could delete the existing RAIDs on both the host server and the expansion array, then combine all drives into one high-capacity storage system.

This configuration reduces administrative complexity and overhead, but the failure of any one unit in the system (due to a cable coming loose, for example) will render the entire RAID inaccessible. This configuration also increases the potential for multiple drive failures in a single RAID. See “RAID Groups” on page 54 for information on how to avoid this.

Cautions

- Host server disk drives and expansion array disk drives are logically interchangeable, but they are not physically interchangeable. That is, you cannot physically take a disk drive from an expansion array and place it in a host SnapServer. SnapServer disk drives contain GuardianOS-specific data that is lacking on expansion array disk drives.
- Do not mix drives of different capacity in a RAID 1, 5, 6, or 10. The redundancy schemes in these RAID types limit capacity usage in all member drives to the capacity of the smallest member disk drive. For example, if a RAID consists of one 160 GB disk drive and three 250 GB disk drives, the RAID can use only 160 GB on each disk drive. In this case, the total RAID capacity is approximately 640 GB (4 x 160) rather than the expected 910 GB (160 + [3 x 250]).
- Do not mix drives of different rotational speeds in the same column. See “Adding New Disk Drives to Increase Capacity” on page 68 for illustrations of supported and unsupported drive configurations.

Integrating Orphan Expansion Units

Expansion units that have been discovered by GuardianOS (e.g., are physically connected to the SnapServer) but have not been integrated with the SnapServer are listed in the Orphan Expansion Units table:

Property	Description
Expansion Unit	A description of the unit
Status	The status of the unit (e.g., orphan)
Serial Number	The expansion unit’s serial number
Origin	The serial number of the server with which the expansion unit was last incorporated

If you want to use the expansion unit with the SnapServer, click the check box next to the orphan expansion unit you want to integrate, and click **OK**.

Caution Before integrating an orphan expansion unit, be sure that it is compatible with the SnapServer (e.g., data on the expansion unit is compatible with the SnapServer configuration, Unicode settings are the same, etc.).

Disks and Units

The Disks/Units screen is a graphic representation of RAID configuration and disk status on your server. The legend explains the meaning of each icon.

- Move the mouse over a RAID set name to highlight all disks within the RAID set.
- Click a RAID set name to view or edit the RAID set.
- Click a disk icon to view disk details.
- Click a unit's LED icon to flash the unit's LEDs for identification.

  Note The LEDs will continue to flash for five minutes. To stop a unit's flashing LED, click that unit's LED icon with a red 'X'. To stop flashing LEDs for all units, click the link at the bottom of the Disks/Units page.

Expansion arrays, if attached to your server, will also be displayed here.

Note If GuardianOS detects an expansion unit that is not integrated with the SnapServer, a warning displays across the top of the Disks/Units screen with a link to information about the orphan expansion unit.

- Adding New Disk Drives to Increase Capacity

Replacing Disk Drives on a RAID

This section describes how to safely remove and replace drives to a degraded RAID. After a fresh drive is inserted into the drive bay, you must use the Administration Tool to add it to a RAID.

How RAIDs React to Disk Drive Removal

- **RAID 0 (nonredundant) —** Removing a disk drive from a RAID 0 causes the RAID to fail. This action renders any data residing on its drives inaccessible and is not recommended. If a RAID 0 disk drive is inadvertently removed, reinserting it should restore file access.
- **RAID 1, 5, 6, or 10 (redundant) —** Removing a disk drive from a two-drive RAID 1 or a RAID 5, 6, or 10 places the RAID into degraded mode. While operating in degraded mode, users can access or even update data. However, the array loses its redundant characteristics until all drives of the array are available and operating properly (except for RAID 6, which can tolerate a two-drive failure before it loses redundancy).

Note If you configure a RAID 1, 5, 6, or 10 with a hot spare, the array automatically starts rebuilding with the hot spare when one of the disk drives fails or is removed.

Note Failed drives cannot be added back in to a RAID.

Adding Disk Drives to a RAID

This section describes how to safely add drives to an existing RAID 1, 5, 6, or 10. On SnapServers, after a fresh drive is inserted into a drive bay, you must use the Administration Tool to add it to a RAID.

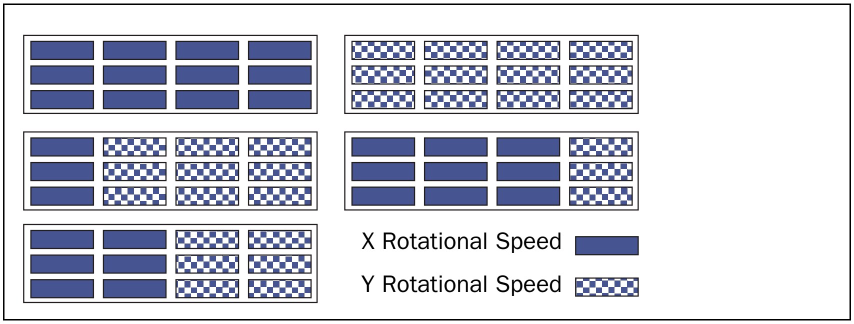
How RAIDs React to Disk Drive Additions

- **RAID 0** (nonredundant) — You cannot add a drive to a RAID 0. To reconfigure a RAID 0, you must delete the RAID and then recreate it.
- **RAID 1** (redundant) — You can add a new drive to a RAID 1 as either a hot spare or as a new member. Adding a disk drive to a RAID 1 does not add storage capacity. The new member simply creates an additional copy of the original drive.
- **RAID 5, RAID 6, RAID 10** (redundant) — You can add a hot spare to a RAID 5; RAID 6, or RAID 10. However, you cannot add a new drive as a new member.

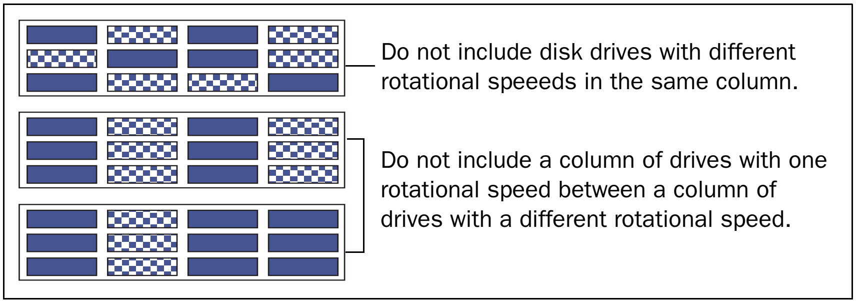
Adding New Disk Drives to Increase Capacity

For those servers and expansion arrays that ship with fewer than the maximum number of disk drives, additional drives can be added to the server or expansion array to increase capacity. Drives of different rotational speed (e.g., SAS and SATA drives) can be combined in the same server. However, they cannot be combined in the same column, and it is recommended that columns of same-type drives be grouped together. If you are combining drives with different rotational speeds, use the figures below to plan where to place the disk drives.

Recommended Disk Drive Configurations



Unsupported Disk Drive Combinations



Do not include disk drives with different rotational speeeds in the same column.

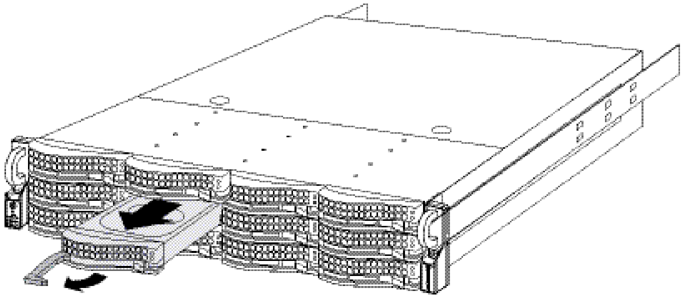
Do not include a column of drives with one rotational speed between a column of drives with a different rotational speed.

To Add New Disk Drives to Increase Capacity on a SnapServer N2000 or E2000

1 Review the Recommended Disk Drive Configurations and Unsupported Disk Drive Combinations, and determine which drive slots to populate with new disk drives.

2 Remove the bezel by pressing the latch on the left side of the bezel (as you face it) and gently pulling to release the left side from the chassis. With the left side open, pull the bezel to the left to release the right side pegs and remove the bezel.

3 Press the latch on the right side of the disk drive blank to release the front lever. Grasp the lever and pull to remove the drive blank from the chassis.



4 With the drive carrier lever open, slide the new disk drive into the chassis. Once the drive is pushed all the way into the chassis, close the drive carrier lever and press until it locks into place.

5 Repeat Steps 3 and 4 for each drive blank you replace with a disk drive.

6 Replace the bezel by sliding the pegs on the right side of the bezel into the holes in the chassis. With the left-side latch pressed in, fit the left side of the bezel onto the front of the chassis. When the bezel is positioned correctly, release the latch to lock the bezel in place.

Hot Swapping Disk Drives

The term *hot swap* refers to the ability to remove and add components to a system without the need to turn off the server or interrupt client access to files.

When to Hot Swap Disk Drives

When available storage space is not at a premium, most administrators prefer to configure a RAID with a hot spare that automatically takes the place of a failed drive. This solution assures that client access to file systems is not interrupted. In environments where configuring a hot spare is not possible, you may need to hot swap a drive.

Hot Swapping Disk Drives

You can hot swap disk drives on SnapServer RAID 1, 5, 6, or 10 by following the two basic steps outlined next:

1 **Remove the failed drive from its bay, and insert the new drive.**

The procedures for the physical removal and replacement of a disk drive for SnapServers are explained in the following sections.

Note If you have enabled the *automatic incorporation of an unused disk* feature, the drive you insert (a raw drive, a drive with a non-GuardianOS partition, or an unassigned GuardianOS-partitioned drive) will be automatically incorporated into the RAID. Skip Step 2.

2 **Configure the new drive as part of the RAID.**

When you remove a drive from a SnapServer, the affected RAID transitions to degraded mode. It remains in degraded mode until the newly inserted drive is configured as a member of the RAID via the Administration Tool. For details on this procedure, see “Adding Disk Drives to a RAID” on page 68.

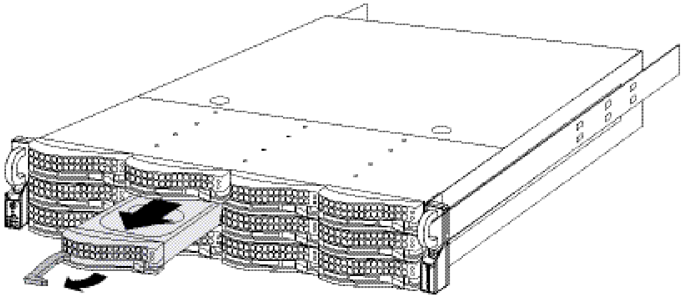
Replacing a Disk Drive on a SnapServer N2000 or E2000

When the bottom LED on the disk drive is red, the drive has failed or is not working properly.

1 Remove the bezel by pressing the latch on the left side of the bezel (as you face it) and gently pulling to release the left side from the chassis.

2 With the left side open, pull the bezel to the left to release the right side pegs and remove the bezel.

3 Press the latch on the right side of the disk drive to release the front lever. Grasp the lever and pull to remove the drive from the chassis.



4 With the drive carrier lever open, slide the new drive into the chassis.

5 Once the drive is pushed all the way into the chassis, close the drive carrier lever and press until it locks into place.

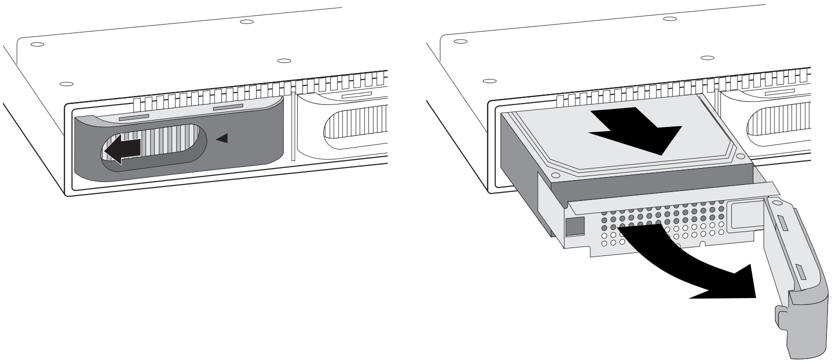
6 Replace the bezel by sliding the pegs on the right side of the bezel into the holes in the chassis.

7 With the left-side latch pressed in, fit the left side of the bezel onto the front of the chassis. When the bezel is positioned correctly, release the latch to lock the bezel in place.

Replacing a Disk Drive on a SnapServer 410

When the status LED is amber and the activity LED is off, the drive has failed or is not working properly.

1. Remove the front bezel by pressing in the latches on each side of the bezel and pulling the bezel away from the chassis.
2. On the closed handle of the failed disk drive, insert your finger into the handle slot and pull out to open the handle.



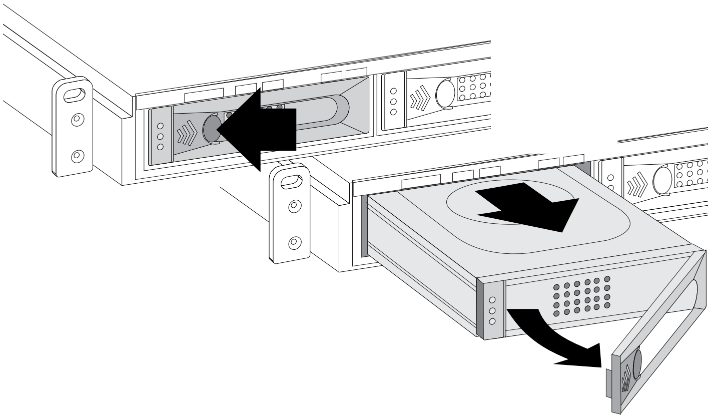
3. Pull to remove the drive from the chassis.
4. Open the handle of the new drive. If the handle is closed, you cannot insert the disk drive completely into the bay.
5. Insert the new disk drive, making sure you push it forward until it is firmly seated and the handle begins to swing closed. Then close the handle until it clicks into place to completely seat the drive to its connection.
6. Replace the front bezel.

Replacing a Disk Drive on a SnapServer 510, 520, 550, 620, 650, or Snap Expansion S50

When the status LED is amber and the activity LED is off, the drive has failed or is not working properly.

1 Remove the front bezel (if applicable) by pressing in the latches on each side of the bezel and pulling the bezel away from the chassis.

2 On the closed handle of the failed disk drive, press the button in and to the left to release the latch.



3 Open the handle and pull to remove the drive from the chassis.

4 Release the latch on the new drive and open its handle. If the handle is closed, you cannot insert the disk drive completely into the bay.

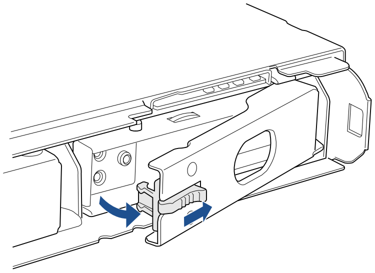
5 Insert the new disk drive, making sure you push it forward until it is firmly seated and the handle begins to swing closed. Then close the handle until it clicks into place to completely seat the drive to its connection.

Note Be sure to push firmly on the drive to securely seat it in the drive bay before you close the handle. You should hear a click to indicate the drive has been inserted as far as it can go.

6 Replace the front bezel.

Replacing a Disk Drive on the SnapServer 4200, 4500, or Snap Disk 10

When the drive's power LED is amber and the activity LED is off, the disk drive has failed or is not working correctly.

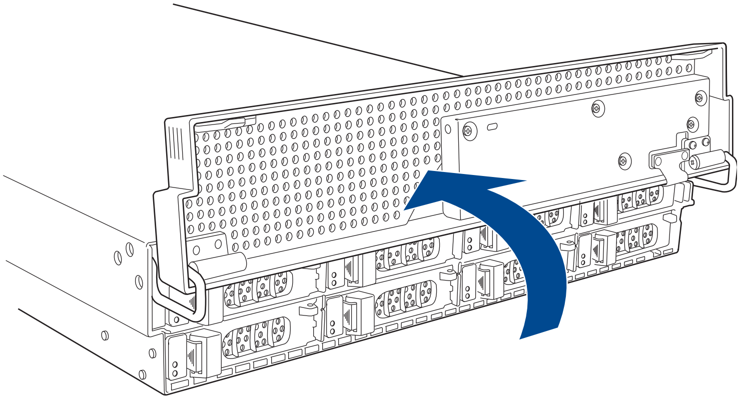


1 Remove the front bezel. With a hand on each latch, slide both latches on the front bezel toward the center. While holding the latch in the release position, pull the bezel away from the chassis.
2 On the closed handle of the failed disk drive, press the latch to the right.
3 To remove the failed disk drive, pull its handle.
4 Release the latch on the new disk drive and open its handle. If the handle is closed, you cannot insert the disk drive completely into the bay.
5 Insert the new disk drive. Make sure you push it forward completely before you press the handle into place.
6 Replace the front bezel.

Replacing a Disk Drive on the SnapServer 18000

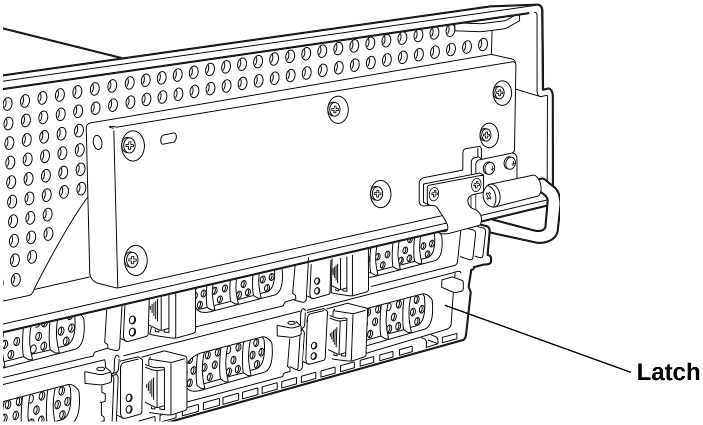
When the status LED is amber and the activity LED is off, the drive has failed or is not working properly.

1 Open the font panel.



2 Remove the failed disk drive by pressing the latch on the handle of the drive and pulling the handle.

3 Release the latch on the new disk drive and open its handle. The handle must be open for you to insert the disk drive all the way into its bay. Insert the new disk drive into the empty drive bay, pushing it all the way forward before you close the handle.

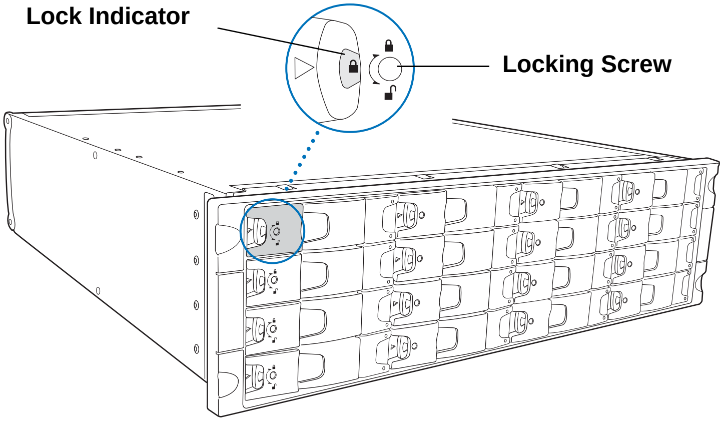


4 Close the font panel.

Replacing a Disk Drive on an SD30SA

When the status LED is green and the fault LED is amber, the drive has failed or is not working properly.

1 Using the Torx driver (T-10) provided, unlock the disk drive by turning the lock screw counterclockwise until the red padlock icon in the lock indicator is no longer visible.



2 To release the handle, press the latch. The handle springs forward.

3 Grasp the handle and remove the failed disk drive by pulling it towards you.

4 To insert a new disk drive, release the carrier handle by pressing the latch and insert the carrier all the way into the enclosure.

5 Once the carrier is in the enclosure, close the handle until you hear a click.

6 Using the Torx driver, lock the carrier into place by turning the lock screw clockwise until the red padlock icon is visible.

iSCSI Disks

Internet SCSI (iSCSI) is a standard that defines the encapsulation of SCSI packets in Transmission Control Protocol (TCP) and their transmission via IP. On SnapServers, an iSCSI disk is based on an expandable, RAID-protected volume, but appears to a client machine as a local SCSI drive. This storage virtualization frees the administrator from the physical limitations of direct-attached storage media and allows capacity to be expanded easily as needed. Unlike standard SnapServer volumes, SnapServer iSCSI disks can be formatted by the iSCSI client to accommodate different application requirements.

Connectivity to the iSCSI disk is established using a software package or PCI card, known as an initiator, that must be installed on a client machine. The initiator sees the SnapServer as a "target portal" and an iSCSI disk as a "target."

To use the SnapServer as an iSCSI target, you need to configure iSCSI on both the client initiating the iSCSI connection, and on the SnapServer. Use the information presented here in conjunction with the documentation supplied with your initiator to install, configure, and connect the iSCSI initiator(s) to the SnapServer.

iSCSI Disk Limitations

- The iSCSI protocol limits the size of any iSCSI disk to 2TB.
- The GuardianOS can maintain up to 256 iSCSI disks.

For Additional Information

The following resources provide further information you may need to plan and complete your iSCSI implementation.

- **SnapServer Online Help:** Available from the **Storage > iSCSI** screen, the online help provides details on creating and managing iSCSI disks on SnapServers.
- **RFC3720 — Internet Small Computer System Interface (iSCSI):** Detailed specification for the iSCSI protocol, available from http://www.ietf.org.
- **RFC4171 — Internet Storage Name Service (iSNS):** Detailed specification for the iSNS protocol, available from http://www.ietf.org.
- **The Microsoft iSCSI Software Initiator User's Guide:** (uguide.doc) This document is packaged with the initiator download and installs to the default location, usually: C:\Windows\iscsi\uguide.doc. It can also be downloaded from the Microsoft web site.

- **The SANSurfer iSCSI HBA CLI Application Users Guide:** This document is available for download on the QLogic web site at http://support.qlogic.com/support/drivers_software.asp.
- **The RedHat or Novell (SuSE Linux) web sites:** Information on configuring the Linux in-box initiators can be found by searching for *iSCSI* on the RedHat or Novell web sites.
- **The Novell NetWare Administrator's Guide:** This document is available for download on the Novell web site.
- **The VMware Server Configuration Guide:** This document is available for download on the VMware web site.
- **Readme files and Help menus:** For Solaris 10 and operating systems using Open iSCSI (SuSE 10, RedHat 4/5, and CentOS 5), the readme files and help menus provide information on installing and configuring iSCSI.

Configuring iSCSI Initiators

Overland Storage has qualified a number of software initiators, PCI cards, and drivers to interoperate with SnapServers. See the iSCSI support page on our website for the latest information on supported versions of these software and hardware initiators.

The following sections briefly describe the initiators supported by GuardianOS and some of the more common configuration options.

- iSCSI Configuration for Microsoft Windows using MS Initiator
- Configuring the QLogic QLA4010 and QLA4050/52c iSCSI Initiators for Microsoft Windows
- iSCSI Configuration for Linux and UNIX
- iSCSI Configuration for Novell NetWare
- iSCSI Configuration for VMware
- iSCSI Configuration for Mac

iSCSI Configuration for Microsoft Windows using MS Initiator

Installation and configuration information is included with the MS Initiator download (*uguide.doc*). It can also be downloaded from the Microsoft web site.

Before implementing iSCSI using MS Initiator, please consider the following:

- On pre-Vista operating systems, Microsoft does not support "dynamic" disks for use with the Microsoft iSCSI initiator. Overland Storage recommends using the QLogic QLA4010/4050, which supports “dynamic disks”, or using only "basic" disks with the Microsoft initiator to avoid unexpected behavior and possible data loss when using the MS initiator to connect to iSCSI targets in a SnapServer.
- To extend the size of a basic disk on pre-Vista operating systems, use the diskpart.exe utility as described in “Using the Microsoft Diskpart Utility to Grow iSCSI Basic Disks” on page 82 or refer to Microsoft KB article 325590. The Microsoft knowledgebase can be found at http://support.microsoft.com. On Vista, Windows 2008, and Windows 7 systems, use the disk management tool to resize the disks.

Configuring Microsoft Services Installed on iSCSI Disks to Start Automatically

iSCSI technology allows SnapServers to host the data files for applications that otherwise require local disk storage, such as MS SQL Server 2000 and Exchange Server 2003. If you use the Microsoft initiator on Windows XP, Windows 2003, Vista, Windows 7, or Windows 2008 server, services installed on iSCSI disks will start up automatically by default once you have configured them to persistently reconnect. On the Windows 2000 server, however, you must edit the Windows registry to make the service dependent on the iSCSI Initiator Service.

Caution Use the Registry Editor with caution. Changes suggested by Overland Storage should be evaluated by qualified technical staff to ensure that they do not affect the proper functionality of the Windows implementation, installed applications, or other components on the Windows system whose registry is being modified. The result of any modifications to the Windows registry can vary, and implied outcomes of any modification suggested by Overland Storage are NOT guaranteed, and may not be supported.

Overland Storage strongly recommends backing up your registry before making any modifications. Please see Microsoft Knowledge Base article 322755 (Windows 2000) for details on backing up and restoring the Windows registry.

Configuring the Server to Persistently Connect

1. Create an iSCSI disk on the SnapServer (see “Creating iSCSI Disks” on page 91).
2. From the Target tab of the Initiator’s Property dialog box, select the Target, click the **Logon** button, check the **Automatically restore this connection when the**

system reboots box to make this a persistent target, then click **OK** to log in to the SnapServer target.

3 Use the Disk Administrator to configure all volumes on top of the disks.

4 From the Bound Volumes/Devices tab on the Property dialog box, click **Bind All** to allow the iSCSI service to configure the list of persistent volumes. If you are running Windows XP, Windows 2003 Server, Vista, Windows 7, or Windows 2008 Server, your iSCSI disks will now start automatically on reboot. If you are running Windows 2000 Server, you must continue to the following procedure and edit the registry to make services dependent on the iSCSI Inititator service.

Editing the Windows Registry for MS Exchange Server or MS SQL Server (Windows 2000 only)

1 Install Exchange Server 2003 and configure it to use the iSCSI disk as the location to store database files.

2 On a Windows workstation running Windows 2000, enter the following on the command line:

```
regedt32
```

3 Navigate to the Key:

a For Exchange Server:

`HKey_Local_Machine > System > Current Control Set > Services > lanmanserver`

b For SQL Server:

`HKey_Local_Machine > System > Current Control Set > Services > MSSQLServer`

4 If the value `DependOnService` already exists, double-click it. If it does not, create it:

a Select **Add Value** from the Edit menu to open the Add Value dialog box.

b In the **Name** field, enter:

`DependOnService`

Click **OK**.

5 In the Data box that opens, enter:

`MSiSCSI`

Click **OK**, and then close the registry.

6 Reboot the Windows server.

Configuring Shares to iSCSI Disks

When using the Microsoft initiator, shares to iSCSI disks may not automatically reconnect when the Windows system hosting the shares is rebooted. There are two methods to resolve this issue:

- Share an iSCSI target that has an assigned drive letter. This method requires changes to the Windows registry and is described in Microsoft Knowledgebase article #870964.
- Mount the iSCSI disk to a folder on an existing NTFS volume as described in "Mounting an iSCSI Disk Without a Drive Letter". This method does not require changes to the Windows registry and is described below.

Mounting an iSCSI Disk Without a Drive Letter

To complete this procedure, you must create and format an iSCSI target on the SnapServer and connect to this iSCSI disk using the Microsoft initiator. You must also have an existing NTFS volume on a local disk within the Windows server, initiating the connection.

1. Right-click My Computer and select **Manage**.
2. The new formatted volume will appear in the Disk Management window.
3. Right-click the **New Volume** and select **Change Drive Letter and Paths...**.
4. Click **Remove** in the Change Drive Letter and Paths for (New Volume) dialog, and click **Yes** to confirm drive letter removal.
5. Right-click the **New Volume** again and select **Change Drive Letter and Paths...**.
6. Select **Add** in the Change Drive Letter and Paths for (New Volume) dialog.
7. In the Add Drive Letter or Path dialog, select **Mount in the following empty NTFS folder**.
8. Create a folder or enter the path to the one that will be shared from the Windows server and select **OK**.
9. Select **OK** in the Add Drive Letter or Path dialog. This will return you to the Disk Management window.

   You will see the icon of a disk in place of the folder icon in the File Management window.
10. Create a share to the iSCSI disk in the standard method, then reboot the Windows machine and verify that the share is persistent.

Configuring Dynamic Disks to Persistently Reconnect

On pre-Vista operating systems, when iSCSI targets are configured as dynamic disks, the Microsoft iSCSI initiator connecting to the dynamic disk may fail to connect properly during system boot. Using dynamic disks for iSCSI targets on pre-Vista operating systems is not supported by Microsoft. For more information, see the *Microsoft iSCSI Software Initiator User's Guide,* available on the Microsoft web site (*uguide.doc*).

Using the Microsoft Diskpart Utility to Grow iSCSI Basic Disks

In a Microsoft environment, *basic disk* is the simplest configuration method for an iSCSI disk. Basic disks are given the highest priority at both system and application services startup to ensure proper initialization.

For Vista, Windows 7, and Windows 2008 Server, use the Disk Management utility. For Windows 2003 Server, Windows 2000 Server, and Windows XP, Microsoft offers a command line utility called Diskpart that allows you to expand basic disks. This utility ships with Windows 2003 Server, and is available for download for Windows 2000 Server and XP. Additional details on the Diskpart utility can be found in Microsoft Knowledge Base article Q300415 (http://support.microsoft.com/kb/300415).

Preparing to Expand a Microsoft Basic iSCSI Disk

The following steps must be taken to prepare for the expansion of a basic iSCSI disk from a Windows host:

1. Using the Microsoft Services GUI, stop all application services that are using the volume you intend to expand.
2. If it is not already installed, load the Diskpart utility on the host machine that is running the iSCSI initiator

   Note If Diskpart is already installed, you will get the appropriate response when entering `diskpart -` at the command line. If the command returns `command not found,` locate diskpart on the Microsoft website, download the utility, and install it on the local host.
3. Log off the iSCSI volume that is to be expanded.
   - Open the Microsoft initiator tool.
   - Under Connected Targets, highlight the specific iSCSI disk(s) you want to expand.
   - Click **LogOff**. This will log you off the specific target.

4 Verify that you have additional space available on the SnapServer to expand an existing volume

- Open the browser-based Administration Tool for the SnapServer from a client on the network.
- Navigate to **Storage > iSCSI**.
- Select the iSCSI disk you intend to expand.

Note If you have not disconnected from the iSCSI disk at the host, you will be unable to proceed to the configuration page.

- From the configuration screen, ensure that you have additional space on the volume to expand the selected iSCSI disk.
- Make changes to the iSCSI disk size as desired.
- Click **OK**. The disk should now reflect the larger size.

Expanding the Basic Disk on the Microsoft Host

1 Open the Microsoft initiator tool.

2 Under Available Targets, highlight the specific iSCSI disk(s) you expanded in the previous procedure.

3 Click **LogOn**. This will connect the initiator to the selected iSCSI target.

4 Close the Microsoft initiator tool.

5 Open the Disk Management tool by right-clicking My Computer and selecting **Manage**. In the Computer Management GUI, select **Disk Management**.

Note The disk will automatically reattach, and the additional expanded space in the iSCSI disk will appear as unallocated space on the same disk.

Expanding an iSCSI Volume using the Microsoft Diskpart Utility

1 In the Start menu, select **Run** and enter `CMD` in the Run dialog to open a command-line window.

2 Enter the command:

```
diskpart
```

3 To show all the available disks on the host, enter:

```
list disk
```

4 Identify the specific disk you are expanding.

5 To show all the available volumes on the host, enter:

```
list Volume
```

6 Identify the specific volume you are expanding.

7 Enter:

```
select disk n
```

where *n* is the disk number that Diskpart indicated from the list command.

8 Enter:

```
select Volume n
```

where *n* is the volume number that Diskpart indicated from the list command.

9 Enter

```
extend size=n
```

where *n* is the number of megabytes you want to expand the disk.

For example, if you are adding 10 GBs to an existing disk of 100 GBs, use the following command:

`extend size=10240` (the number is in megabytes, 1024MBs = 1GB)

Note The Disk Management GUI will show the newly expanded disk size.

10 Exit the Computer Management tool.

11 Restart the necessary application services.

Configuring the QLogic QLA4010 and QLA4050/52c iSCSI Initiators for Microsoft Windows

QLogic's QLA4010 and QLA4050/52c are iSCSI adapters that appear as a SCSI adapter instead of a network adapter in Windows Device Manager. Before the QLA4010 or QLA4050/52c can successfully connect to iSCSI targets, you must:

- Set initiator parameters (for example, initiator name, alias, IP address).
- Enter target information (for example, target portal information and target iSCSI name).

You can use either the SANSurfer Management application that came with the QLA4010/4050/4052c or Microsoft’s iSCSI initiator applet to set initiator parameters and enter target information. Follow the instructions in the documentation to install and configure the adapter.

iSCSI Configuration for Linux and UNIX

Before implementing iSCSI on Linux or UNIX systems, consider the following:

- The QLogic QLA4010/4050/4052c hardware initiator supports Red Hat Enterprise Linux 3, QU5; Red Hat Enterprise Linux 4, QU1; and SuSE Linux Enterprise Server 9, SP3. This initiator provides CHAP authentication and can connect to multiple targets simultaneously. The SANSurfer utility is included with the HBA to initiate, monitor, and change iSCSI targets using its text-based user interface.
- The Cisco-based in-box iSCSI software initiators for Linux support Red Hat Enterprise Linux 3, QU6, Red Hat Enterprise Linux 4, QU2, and SuSE Linux Enterprise Server 9, SP3.
- The Open iSCSI-based in-box iSCSI software initiators for Linux support RedHat Linux 5 QU1 and higher, SuSE Linux Enterprise Server 10, SP1 and higher and CentOS 5.0 and higher.
- The Open iSCSI-based in-box iSCSI software initiator for UNIX supports Solaris 10 U4.

Installation and configuration information for the QLogic QLA4010/4050/4052c HBA is included with the adapter and is also available for download from the QLogic website. Information about the in-box iSCSI intitiators is available from the RedHat, Novell (SuSE Linux), and Sun Microsystems web sites.

Using CHAP Authentication to Enable Multiple Linux Systems to Share iSCSI Disks Securely on a SnapServer

You can use CHAP authetication to enable multiple Linux systems with in-box initiators to share different iSCSI disks on a SnapServer or SnapServers. To do this, you would set up different Usernames and Passwords for a DiscoveryAddress.

For example, on a SnapServer (IP address:192.3.2.193), iSCSI disks can be configured for System A and System B. With CHAP enabled, set the System A Username to *a*, and set the Password to *PasswordForA*. Then, for system B, set the Username *b*, and set the Password to *PasswordForB*. The configuration will look like the following:

In System A's `/etc/iscsi.conf`, enter the following:

```
DiscoveryAddress=192.3.2.193
  Username=a
  Password=PasswordForA
```

In System B's `/etc/iscsi.conf`, enter the following:

```
DiscoveryAddress=192.3.2.193
  Username=b
  Password=PasswordForB
```

System A and B can connect to their own iSCSI disks on the same SnapServer (IP address 192.3.2.193) without the possibility of data corruption caused by sharing the same iSCSI disk.

iSCSI Configuration for Novell NetWare

Consider the following information before implementing iSCSI on NetWare servers:

- NetWare 6.5 with SP1 for NetWare is required, and the iSCSI packages must also have been installed using the Custom Install method to utilize the NetWare iSCSI initiator.
- The server initiating the connection should be a P-III or higher with a minimum of 512MB of RAM and a GbE adapter. To validate the NetWare server's ability to communicate with the SnapServer, ping the SnapServer from the NetWare server.
- With GuardianOS 5.0, CHAP authentication is supported on NetWare 6.5, SP7.

  Note CHAP authentication is not supported on versions of NetWare 6.5 earlier than SP7, nor is it supported on pre-GuardianOS 5.0 systems.
- iSCSI implementation requires configuration using the NetWare Remote Manager or the command line in the Server Console.

For more information regarding installation and configuration of required NetWare components, refer to the documentation included with the Novell initiator distribution.

iSCSI Configuration for VMware

Note GuardianOS 4.2/4.3, SP2 or higher is required to configure iSCSI disks with the VMware Initiator.

When you install VMware ESX Server or vSphere Server, the iSCSI Initiator is automatically installed.

On connecting to the SnapServer targets, the VMware ESX 3.5 Server initiator will find all iSCSI disks and automatically log into them. If iSCSI disks are shared across multiple servers, you can use CHAP authentication to restrict the number of iSCSI disks the VMware initiator can access. See “Creating iSCSI Disks” on page 91 for more information. The VMware vSphere 4.0 Server initiator provides the option for

Static Discovery, allowing you to enter the IP addresses of only those targets you want the VMware initiator to access.

For more information regarding installation and configuration of required VMware components, refer to the documentation included with the VMware Server installation.

Using the VI Client to Configure iSCSI Services

Follow the instructions in the *VMware Server Configuration Guide*, available from

http://www.vmware.com

to configure your iSCSI service. Use the VI Client to:

1 Configure the Service Console that connects to the VMware host.

2 Create the VMKernel on the NIC used for the iSCSI connection.

3 Enable the iSCSI software initiator, set up target IP addresses, and configure CHAP authentication (if desired). Rescan if necessary to see the new iSCSI service.

   Note On pre-VMware ESX 3i systems, you must open a port in your security profile to enable the iSCSI port. From the Configuration tab, select **Security Profile**, click **Properties**, and check the port for the iSCSI Initiator.

4 Use the **Add Storage** option to configure your storage.

iSCSI Configuration for Mac

GuardianOS supports the SmallTree abcSAN iSCSI initiator for use with MacOS 10.5. Download the initiator software from the SmallTree web site, and follow the installation instructions.

Important! If iSCSI is used on a SnapServer with more than one Ethernet port, Mac OS X iSCSI clients can encounter connectivity issues if multiple ports are connected to one or more networks. To avoid these issues, configure the server from **Network > TCP/IP** to enable and connect only one standalone interface or one bonded pair (Load Balance, Failover, etc.) to a single network.

iSCSI Configuration on the SnapServer

iSCSI disks are created on the **Storage > iSCSI** screen of the Administration Tool. Before setting up iSCSI disks on your SnapServer, carefully review the following information.

Isolate iSCSI Disks from Other Resources for Backup Purposes

It is important to isolate iSCSI disks from other resources on the SnapServer for two reasons:

- The file system of an iSCSI disk differs fundamentally from the SnapServer's native file system
- iSCSI disks are managed from client software rather than the SnapServer's Administration Tool

For ease of management and particularly for data integrity and backup purposes, either dedicate the entire SnapServer to iSCSI disks, or if the server is to be used with other shared resources, place the iSCSI disk and the other shared resources on separate volumes.

- **Back up an iSCSI Disk from the Client, not the SnapServer —** An iSCSI disk is not accessible from a share and thus cannot be backed up from the SnapServer. The disk can, however, be backed up from the client machine from which the iSCSI disk is managed.

  Note While some third-party, agent-based backup packages could *technically* back up an iSCSI disk on the SnapServer, the result would be inconsistent or corrupted backup data if any clients are connected during the operation. Only the client can maintain the file system embedded on the iSCSI disk in the consistent state that is required for data integrity.

- **Do Not Use the GuardianOS Snapshots Feature on a Volume Containing an iSCSI Disk —** Running a GuardianOS snapshot on a volume containing an iSCSI disk will abruptly disconnect any clients attempting to write to the server's iSCSI disk and the resulting snapshot may contain inconsistent data. Supported Windows servers can create a native snapshot of a SnapServer iSCSI disk using VSS (see "Configuring VSS/VDS for iSCSI Disks" on page 93 for more information).

iSCSI Multi-Initiator Support

The Support Multi-Initiator check box allows two or more initiators to simultaneously access a single iSCSI target. Multi-Initiator Support is designed for use with applications or environments in which clients coordinate with one another to properly write and store data on the target disk. Data corruption becomes possible when multiple initiators write to the same disk in an uncontrolled fashion.

Note GuardianOS v5.1 and later support Windows 2003 and Windows 2008 Server failover clustering.

The warning message *Uncontrolled simultaneous access of multiple initiators to the same iSCSI target can result in data corruption. Only enable Multi-Initiator Support if your environment or application supports it* occurs when the checkbox for Support Multi-Initiator is selected. It functions as a reminder that data corruption is possible if this option is used when creating an iSCSI disk.

Write-Cache Options with iSCSI Disks

Note This section refers only to iSCSI disks. For information about configuring write cache on GuardianOS volumes, see “Configuring Write Cache” on page 58.

To ensure the fastest possible write performance, SnapServers can buffer up to 1GB of data to efficiently handle data being transmitted to a SnapServer. This widely accepted method of improving performance is not without some risk. For example, if the SnapServer were to suddenly lose power, data still in cache would be lost.

This risk can be minimized by following industry-standard security precautions, such as keeping servers in a secured location and connecting power supplies to the mains using a network- or USB-based UPS. In most environments, taking these simple precautions virtually eliminates the risk of serious data loss from sudden and unexpected power outages.

Of course, the physical conditions and company policies that guide IT decisions vary widely. Power outages are a common occurrence in some areas, and data protection procedures vary from company to company. Administrators who determine that the risk of data loss, even with security cautions in place, outweighs the significant increase in write performance that write-cache provides, can disable this feature for individual iSCSI disks.

Notes

- Write-cache can be disabled on an iSCSI-disk-by-iSCSI-disk basis. Disabling write-cache for an iSCSI disk does *not* disable write-cache for any other iSCSI disk or any other resources on the SnapServer.
- The opportunity to enable/disable write-cache for an iSCSI disk occurs only when the disk is created; it cannot be toggled at a later date.
- Disabling write-cache for an iSCSI disk does not eliminate *all* potential risk of data loss due to an unexpected loss of power as each disk drive contains its own internal cache of 8 MB or more.

Disconnect iSCSI Disk Initiators before Shutting Down the Server

Shutting down the server while a client initiator is connected to an iSCSI disk appears to the client initiator software as a disk failure and may result in data loss or corruption. Make sure any initiators connected to iSCSI disks are disconnected before shutting down the server.

Ignore the *Volume is Full* Message

When an iSCSI disk is created, the volume allocates the specified capacity to the disk. If all volume capacity is allocated to the iSCSI disk and email notification is enabled, the SnapServer may generate a *Volume is Full* message. This message indicates only that the volume capacity is fully allocated to the iSCSI disk and is not available to other resources. To determine the status of iSCSI disk storage utilization, use the tools provided on the client machine.

iSCSI Disk Naming Conventions

iSCSI disks are assigned formal IQN names. These appear as the iSCSI device names that the user chooses (or types) when connecting from a client initiator to the SnapServer target, and also on the iSCSI Disk details page.

- The format of IQN names for GuardianOS iSCSI disks on the SnapServer is:

  ```
  iqn.1997-10.com.snapserver:[servername]:[diskname]
  ```

  where *[servername]* is the name of the SnapServer, and *[diskname]* is the name of the iSCSI disk on the target SnapServer. For example:

  ```
  iqn.1997-10.com.snapserver:snap123456:iscsi0
  ```

  Note Users with iSCSI disks created in earlier GuardianOS versions will see a shortened IQN name in the following format:

```
iqn.[servername].[iscsidiskname]
```

- The format of IQN names for VSS-based iSCSI disks on the SnapServer is:

  ```
  iqn.1997-10.com.snapserver:[servername]:[diskname].[nnn]
  ```

  where *[servername]* is the name of the SnapServer, *[diskname]* is the name of the iSCSI disk on the target SnapServer, and *[nnn]* is a sequential number starting from 000. For example:

  ```
  iqn.1997-10.com.snapserver:snap123456:iscsi0.000
  ```

- The format of IQN names for VDS-based iSCSI disks on the SnapServer is:

  ```
  iqn.1997-10.com.snapserver:[servername]:[diskname]-snap[n]
  ```

  where *[servername]* is the name of the SnapServer, *[diskname]* is the name of the iSCSI disk on the target SnapServer, and *[n]* is a sequential number starting from 0. For example:

  ```
  iqn.1997-10.com.snapserver:snap123456:iscsi0-snap0
  ```

Creating iSCSI Disks

Navigate to **Storage > iSCSI** to to create, edit, or delete iSCSI Disks on the SnapServer. Be sure to read “iSCSI Configuration on the SnapServer” on page 88 before you begin creating iSCSI Disks.

Note You cannot delete or edit an iSCSI disk until all clients have been disconnected from that disk.

Click **VSS/VDS Access** to add VSS/VDS clients to the SnapServer. See “Configuring VSS/VDS for iSCSI Disks” on page 93 for more information.

To use CHAP authentication

1 Click to put a check in the **Enable CHAP Logon** box.

2 Enter a user name and target secret (password). Both are case sensitive.

   - The user name range is 1 to 223 alphanumeric characters.
   - The target secret must be a minimum of 12 and a maximum of 16 characters.

GuardianOS Support for CHAP Security (Target Only)

CHAP is a network login protocol that uses a challenge-response mechanism to control iSCSI initiator access to an iSCSI target. GuardianOS supports target authentication, in which the initiator must provide the same CHAP user name and password (or "target secret") that was configured on the target SnapServer iSCSI disk. Other forms of CHAP authentication are not currently supported.

To View iSCSI Disk Status Information

You can view iSCSI disk status information from the **Storage > iSCSI** screen.

Label	Description
iSCSI Disk Name	The name of each iSCSI disk
Volume	The volume on which the iSCSI disk was created
Status	Current condition of the iSCSI disk: • *OK* — The iSCSI disk is online and accessible. • *Not Mounted* — The iSCSI disk is offline.
Active Client	The number of current sessions
Authentication	CHAP or none
Size	The size of the iSCSI disk

To Configure iSNS

Go to the **Network > iSNS** screen, from which you can configure **iSNS**.

To Edit an iSCSI Disk

Click an iSCSI disk name. You can increase (but not decrease) its size and enable or disable CHAP logon.

Note You cannot edit an iSCSI disk if an initiator is connected. The hostname and IQN name of all connected initiators will be displayed.

To Delete an iSCSI Disk

The system will not allow the deletion of an iSCSI disk when clients are connected (the hostname and IQN name of all connected initiators will be displayed). After disconnecting all client initiators, click **Delete**, and then follow the onscreen instructions to delete one or more iSCSI disks.

Configuring VSS/VDS for iSCSI Disks

GuardianOS provides VSS and VDS hardware providers to support Microsoft Volume Shadow Copy Services (VSS) and Virtual Disk Service (VDS) for iSCSI disks.

Note VSS/VDS operations are supported on iSCSI disks created using GuardianOS v5.2 and later.

- The VSS hardware provider provides a mechanism for taking application-consistent native snapshots of iSCSI disks without performing full application (or system) shutdown. A snapshot of an iSCSI disk can be automatically created by a backup job run by a VSS-compatible backup application, so that the job backs up the snapshot volume rather than the main production volume.

  Note VSS iSCSI snapshots are managed by the Windows client and represent the iSCSI disk, not the Snap volume the iSCSI disk resides on. They are not related to GuardianOS snapshots as described in Snapshots.

  Note VSS iSCSI snapshot rollback is not currently supported.

- The VDS hardware provider allows administrators to natively manage SnapServer iSCSI disks, using any VDS compliant management console application.

SnapServers support VSS and VDS on the following platforms:

	VSS	VDS
Windows Server 2003	X	
Windows Server 2003 R2	X	X
Windows Vista		X
Windows Server 2008	X	X

For more information on using VSS and VDS, see the Online Help.

Note RAID types listed in *Storage Manager for SANs* when creating an iSCSI disk reflect the types of RAIDs already configured on the SnapServer. Once a RAID type is selected, the SnapServer automatically chooses a SnapServer RAID of the selected type and volume to create the iSCSI disk on.

Share and File Access

SnapServer has implemented features to accommodate the disparate methods used by the SMB and NFS protocols for sharing data. At the share level, administrators can assign read-write or read-only share access to individual Windows (and local) users and groups. Administrators can also edit the NFS *exports* file to control how shares are exported to NFS client machines.

The SMB and NFS protocols also part ways in their handling of file-level permissions. Administrators can choose to apply Windows or UNIX-style file-level permissions to entire volumes or to directories at the root of a volume (aka SnapTree directories). These security-based directory structures are referred to as SnapTrees.

File and directories in a Windows SnapTree can have either a Windows or UNIX security personality, depending on the network protocol used to create the file or change permissions on it. Files in a UNIX Snap Tree always have the UNIX security personality and can only be set by NFS clients.

Topics in Share Access and File Permissions:

- Configuring Share and Folder Security Overview
- Components and Options
- SnapTrees and Security Models
- ID Mapping
- Shares
- Configuring Share Access
- Creating Home Directories
- Windows ACLs
- Security Guides

Configuring Share and Folder Security Overview

SnapServers support file access in Windows, UNIX, and Apple networks, as well as access via FTP and HTTP. Although the GuardianOS runs on an optimized Linux kernel and has many Linux characteristics, the cross-platform features make it very different than a pure Linux distribution. Systems running GuardianOS are storage appliances dedicated to file services. Administrators should not expect the same behavior as a pure Linux system when administering the SnapServer.

By default, volumes are created with the Windows/Mixed security model (Windows-style ACLs for files created by SMB clients and UNIX-style permissions for files created by other protocols and processes), and allow all users to create, delete, and configure permissions on their own files and to access files and directories created by other users.

New shares are created by default with full read-write access to all users, subject to the file system permissions on the share target directory. The first step to securing a SnapServer is to specify access at the individual share level. Administrators can assign Read/Write or Read-Only share access to individual Windows (and local) users and groups.

Security permissions that have been applied to files and folders can be viewed from the *Web View* page of the Admin Tool. For users with admin rights, a key icon 🔑 appears next to each file and folder in the share. Clicking this icon displays a popup box with security information about the file or folder.

Hidden Shares

There are three ways a share can be hidden in GuardianOS:

- Name the share with a dollar-sign ($) at the end. This is the traditional Windows method of hiding shares; however, it does not truly hide the share since Windows clients themselves filter the shares from share lists. Other protocols can still see dollar-sign shares.
- Hide the share from all protocols (except NFS) by navigating to **Security > Shares > Create Share > Advanced Share Properties** and selecting the **Hide this Share** check box, or by selecting a share, clicking to expand **Advanced Share Properties**, and selecting the **Hide this Share** check box. When a share is hidden this way, the share is invisible to clients, and must be explicitly specified to gain access.

  Note Hidden shares are not hidden from NFS, which cannot access invisible shares. To hide shares from NFS, consider disabling NFS access to the hidden shares.

- Disable individual protocol access to certain shares by navigating to **Security > Shares > Create Share > Advanced Share Properties** and enabling/ disabling specific protocols, or by selecting a share, clicking to expand **Advanced Share Properties**, and enabling/disabling specific protocols.

File and Directory Permissions

GuardianOS supports two "personalities" of file system security on files and directories:

- UNIX: Traditional UNIX permissions (rwx) for owner, group owner, and other.
- Windows ACLs: Windows NTFS-style file system permissions. Introduced in GuardianOS 5.0, Windows ACLs fully support the semantics of NTFS ACLs, including configuration, enforcement, and inheritance models (not including the behaviour of some built-in Windows users and groups).

The security personality of a file or directory is dependent on the security model of the SnapTree or Volume in which the file or directory exists (see "SnapTrees and Security Models" on page 100).

Note Files and directories created pre-GuardianOS 5.0 will continue to have the same permissions they had before, and will continue to be enforced as they were. This includes both UNIX permissions and POSIX ACLs. When a Windows user changes permissions on a file or directory created pre-GuardianOS 5.0 with a POSIX ACL, the file will be updated to the new Windows security personality.

Share Level Permissions

Share-level permissions on GuardianOS are applied cumulatively. For example, if the user "j_doe" has Read-Only share access and belongs to the group "sales", which has Read/Write share access, the result is that the user "j_doe" will have Read/Write share access.

Note Share-level permissions only apply to non-NFS protocols. NFS access is configured independently by navigating to the **Security > Shares** page, selecting from the table the NFS Access level for the share, and modifying the client access as desired.

Where to Place Shares

For security and backup purposes, it is recommended that administrators restrict access to shares at the root of a volume to administrators only. All SnapServers are shipped with a default share named *SHARE1* that points to the root of the default volume *vol0*. The share to the root of the volume should only be used by administrators as a "door" into the rest of the directory structure so that, in the event that permissions on a child directory are inadvertently altered to disallow administrative access, access from the root share is not affected. This also allows one root share to be targeted when performing backups of the server. If it is necessary to have the root of the volume accessible, using the Hidden option helps ensure only those that need access to that share can access it.

SnapTrees

SnapTrees are directories that can be configured for the Windows/Mixed or UNIX security model. SnapTrees make a specific directory structure follow the rules of the specified security model, which indicates which file permission personality will be present on files by default, and whether that personality can be changed by users when changing permissions. All top level volume directories, as well as all directories inside the first level of a volume, are considered SnapTrees. For more information, see “SnapTrees and Security Models” on page 100.

NFS Share Access

When controlling share access for NFS clients, administrators can limit client access to the shares independently of share level permissions that apply to other protocols. Access is controlled on a per-share basis. To set the NFS access, navigate to **Storage > Shares**. In the Shares table, click in the **NFS Access** column of the share you want to modify. Changes made on this screen affect the NFS “exports” file within GuardianOS.

Caution If there are multiple shares to the same directory on the disk, and those shares permit access via NFS, they must all have the same NFS export configuration. This is enforced when configuring NFS access to the overlapping shares.

Components and Options

Shares are created and share access is granted using the Administration Tool. File-level permissions are configured from a Windows or UNIX/Linux workstation. The following table summarizes the components, options, and tools available for setting up share and file security on SnapServers.

Component	Options
Security Models (SnapTrees)	Volumes and directories created in the root of a volume have one of two security models: Windows/Mixed or UNIX. The security model determines the rules regarding which security personality will be present on files and directories created by the various protocols and clients, and whether the personality of files and directories can be changed by changing permissions. These directories are referred to as SnapTrees, and their security models can be configured from the **Security > SnapTrees** screen.
Shares	Shares are created on the **Security > Shares** screen. When creating a share, you must set the following options: • **Name** Select a name for the new share. • **Volume** Select a volume from the drop-down list. • **Path** Browse to the directory you want to use as the root of the share or type in the path to the share. If the path does not exist, when you click Browse or OK, you will be asked if you want to create it. • **Security Model** If you create a share pointing to a volume or a SnapTree directory, a security model must be selected. • **Share Access** User access to the share can be restricted or full read/write access. By clicking to expand **Advanced Share Properties**, you can set the following options: • **Hidden Option** The Hidden option allows you to hide a share from clients connecting from SMB, HTTP/HTTPS, AFP, and FTP (but not NFS) protocols. • **Protocol Access** Client access to the share can be restricted to specific protocols. As a security precaution, disable any protocols not needed by users of the share. • **Snapshot Share** The snapshot share allows access (using identical security) to snapshots of the data that the new share references. **Note** The Snapshot share option only appears when Snapshots have been licensed.

Component	Options
Share Access	Share-level access allows users/groups/clients to connect to a share and is configured from the **Security > Share Access** screen. Users and groups known to the system can be given Full Access or Read Only (R) access to the share.
Share NFS Access	The Administration Tool provides a window into the *exports* file for defining how a share is exported to NFS clients.
File Permissions	File-level permissions define what actions users and groups can perform on files and directories, and are set from a Windows client for a Windows SnapTree; and from a UNIX/Linux client for a UNIX SnapTree.

SnapTrees and Security Models

Volumes and directories created on the root of a volume are assigned one of two security models: Windows/Mixed or UNIX. The security model determines the rules regarding which security personality will be present on files and directories created by the various protocols and clients, and whether the personality of files and directories can be changed by changing permissions. These directories are referred to as SnapTrees.

- **Creating a SnapTree Directory —** SnapTree directories are created either from the **Security > SnapTrees** screen in the Administration Tool or from a client from any of the network protocols. SnapTrees created either by clients or in the Web UI will default to the security model of the parent volume.

  Note The security model of a SnapTree directory may differ from the personality of the directory (a Windows/Mixed SnapTree may have the UNIX personality, and vice-versa).

- **Toggling Security Models —** The security model applied to a volume or SnapTree directory can be changed from the **Security > SnapTrees** screen, or when creating a share pointing to a volume root or SnapTree directory. When changing security models, the corresponding personality (i.e., Windows for Windows/Mixed and UNIX for UNIX) is applied to the SnapTree directory itself with a default permission, and can optionally be propagated with a default permission to all files and directories inside the SnapTree.

SnapTree Functionality

The following table describes the behavior of SnapTrees and Security Models.

Function	Description
SnapTree Directory Ownership	Default ownership differs according to the method used to create the SnapTree directory: • **From the client —** For UNIX personality directories, the owner and owning group will be according to the logged-in user. For Windows personality directories, the owner will be the logged-in user, or “Administrators” for directories created by Domain Admins or members of the local admingrp. • **From the Administration Tool** — For UNIX personality directories, the user and group owner will be admin and admingrp. For Windows personality directories, the owner will be the local admingrp (“Administrators”).
Security Personality of Files and Directories	Files and directories created by clients inside SnapTrees will acquire security personality and permissions according to the rules of the SnapTree security model. **Windows/Mixed SnapTree** • Files and directories created by SMB clients will have the Windows security personality. Permissions will either be inherited according to the ACL of the parent directory (if Windows) or will receive a default ACL that grants the user full access only (if the parent is UNIX or has no inheritable permissions). • Files and directories created by non-SMB clients will have the UNIX personality. UNIX permissions will be as set by the client (per the user’s local umask on the client). • The security personality of a file or directory can be changed by any user with sufficient rights to change permissions or ownership. If a client of one security personality changes permissions or ownership of a file or directory of a different personality, the personality will change to match the personality of the client protocol (e.g., if an NFS client changes UNIX permissions on a Windows file, the file will change to the UNIX personality). **UNIX SnapTree** • Files and directories created by non-SMB clients will have the UNIX personality. UNIX permissions will be as set by the client (per the user’s local umask on the client). • Files and directories created by SMB clients will have the UNIX personality. UNIX permissions will be set to a default. • The personality of files and directories cannot be changed on a UNIX SnapTree. All files and directories always have the UNIX personality.

Function	Description
SnapTree File System Permissions	Security model and permissions differ according to the method used to create the SnapTree directory: • From the client: If SMB, permissions will either be according to ACL inheritance (if the parent volume root directory has the Windows security model) or *Full Access* to the owning user only. Permissions for directories created by all other protocols will be set by the client (per the client's umask). • From the Administration Tool: If created in a UNIX volume, permissions will be *777* (rwxrwxrwx). If created in a Windows/Mixed volume, permissions will allow all users to create, delete, and change permissions on files created inside the SnapTree, and will grant full control to administrators.
Toggling Security Models	Changes to a SnapTree's security model can optionally be propagated to the corresponding personality with a default permission to all files and directories underneath the SnapTree. When changing the security model on a SnapTree: • If changing from Windows to UNIX, all files and directories will be changed to be owned by *admin* and *admingrp*, with UNIX permissions of 777(rwxrwxrwx). • If changing from UNIX to Windows, files and directories will be changed to default permissions that allow all users the ability to create and manage their own files and directories and to access other users' files and directories.
Mixing SnapTrees	You can create SnapTrees of different security models on the same volume.

ID Mapping

ID mapping allows users and groups that exist on Windows domains to share user IDs with local or NIS users and groups. This results in the same permissions and quota consumption applying to both the Windows domain user and the local or NIS user. Example:

> John Smith is a local user on a SnapServer, as well as having a user ID on a Windows domain. John's quota for the SnapServer has been set to 200 MB. The administrator of the SnapServer maps the Windows domain user identification for John Smith to the local identification for John Smith, giving both IDs access to John's 200 MB.

Note Search filters without wildcards will search for all entries containing the string you enter in the search field rather than looking for exact matches. For example, if you enter 'abc' as your search criterion, all users and groups containing 'abc' in the name will be identified.

Shares

Shares are created, viewed, edited, and deleted from the **Security > Shares** screen of the Administration Tool. The shares table lists all of the shares on the SnapServer, and describes the share properties. Guidelines for creating shares are provided below. Be sure to review them before configuring shares on the SnapServer.

Property	Description
Share	Name of each share
Volume	The volume the share points to
Path	The directory path on the volume
Access	The user-level access defined for that share: • **Full**—if AllUsers has full access • **Restricted**—If AllUsers does not have full access
NFS Access	The NFS access defined for that share: • **Default**—if all hosts have read-write access • **User**—If not all hosts have read-write access
Protocols	The network protocols enabled for the share (SMB, NFS, AFP, HTTP/HTTPS, FTP/FTPS) **Note** As a security measure, disable any protocols not required for your network environment.
Attributes	Attributes for the share: • **S**—snapshot share • **H**—hidden share • **W**—webroot share

The default share (SHARE1) maps to the root of the volume and grants access to all users and groups over all protocols.

Guidelines

Consider the following guidelines when creating or deleting shares.

Maintain at Least One Share at the Root of Each Volume

A share to the root of a volume is recommended for backup purposes. Security for any share at the root of the volume should be given special consideration. Any user or group that has access to the root of a volume will have access to EVERY file and subdirectory on that volume unless there is a specific ACL in place precluding that access. In general, access to a share at the root of a volume should only be granted to a system administrator or backup operator.

Hidden Shares

A *hidden* share is hidden from clients connecting from the SMB, HTTP, AFP, and FTP (but not NFS) protocols. For example, assume SHARE1 is set as hidden. Windows users will not see the share when viewing the server through Network Neighborhood, or when performing a `net view \\servername` on the SnapServer.

For more information, see "Configuring Share and Folder Security Overview" on page 96.

Snapshot Shares

A *snapshot share* provides access to all current snapshots of a volume. Just as a share provides access to a portion of a live volume, a snapshot share provides access to the same portion of the file system on any archived snapshots of the volume. You create a snapshot share by selecting the *Create Snapshot Share* check box in the course of creating or editing a share.

Security Models, SnapTrees, and Shares

In the course of creating a share that points to a volume or to a directory on the root of the volume (aka SnapTree directory), you must assign a security model to the volume or SnapTree directory. Thereafter, security models for these entities are managed on the **Security > SnapTrees** screens.

NIS Users

When a SnapServer is connected to a UNIX domain, NIS users do not appear in the list of users under **Security > Shares > Access**. NIS user properties cannot be modified from the SnapServer. However, it is possible to assign quotas to NIS users and groups from the **Storage > Quotas** page in the UI.

To Set Up NFS Share Security

Click the link in the **NFS Access** column next to the share you want to configure. The NFS Share Access screen displays. You can configure NFS access to the share using standard Linux "exports" file syntax.

Note If selecting **Create share with Admin-only access...** and if the share has NFS enabled, be sure to configure the NFS Access settings afterward.

Configuring Share Access

The GuardianOS supports share-level as well as file- and directory-level permissions (see “Windows ACLs” on page 107) for all local and Windows domain users and groups.

Share Access Behaviors

Administrators tasked with devising security policies for the SnapServer will find the following share access behaviors of interest:

- **Share access defaults to full control —** The default permission granted to users and groups when they are granted access to the share is full control. You may restrict selected users and groups to read-only access.
- **User-based share access permissions are cumulative —** An SMB, AFP, HTTP, or FTP user's effective permissions for a resource are the sum of the permissions that you assign to the individual user account and to all of the groups to which the user belongs in the Share Access page. For example, if a user has read-only permission to the share, but is also a member of a group that has been given full-access permission to the share, the user gets full access to the share.
- **NFS access permissions are not cumulative —** an NFS user's access level is based on the permission in the NFS access list that most specifically applies. For example, if a user connects to a share over NFS from IP address 192.168.0.1, and the NFS access for the share gives read-write access to ***** (All NFS clients) and read-only access to 192.168.0.1, the user will get read-only access.
- **Interaction between share-level and file-level access permissions —** When both share-level and file-level permissions apply to a user action, the more restrictive of the two applies. Consider the following examples:

  Example A: More restrictive file-level access trumps more permissive share-level access.

Share Level	File Level	Result
Full control	Read-only to FileA	Full control over all directories and files in SHARE1 *except* where a more restrictive file-level permission applies. The user has read-only access to FileA.

Example B: More restrictive share-level access trumps more permissive file-level access.

Share Level	File Level	Result
Read-only	Full control to FileB	Read-only access to all directories and files in SHARE1, *including* where a less restrictive file-level permission applies. The user has read-only access to FileB.

Setting User-based Share Access Permissions

Share permissions for Windows, Apple, FTP, and HTTP users are configured from **Security > Shares** by clicking the link in the **Access** column next to the share you want to configure. Share permissions for NFS are configured and enforced independently. See "NFS Share Access" on page 98 for more information.

User-based share access permissions apply to users connecting over SMB, AFP, HTTP, and FTP. Users and groups with assigned share access permissions appear in the list to the left (*Users/groups with access to...*) and those without assigned access permissions appear in the list to the right (*Users/groups without access to...*).

The default permission granted to users and groups when they are granted access to the share is full access. You may restrict selected users and groups to read-only access.

Share-Level Access Permissions	
Full access	Users can read, write, modify, create, or delete files and folders within the share.
Read-only	Users can navigate the share directory structure and view files.

Creating Home Directories

The Home Directories feature creates a private directory for every local or Windows domain user that accesses the system. When enabling Home Directories (from the **Security > Home Directories** page), the administrator creates or selects a directory to serve as the home directory root. When a user logs in to the server for the first time after the administrator has enabled Home Directories, a new directory named after the user is automatically created inside the home directory root, and is configured to be accessible only to the specific user and the administrator.

Depending on the protocol, home directories are accessed by users either via a user-specific share, or via a common share pointing to the home directory root.

Home directories are supported for SMB, NFS, AFP, HTTP/HTTPS, and FTP/FTPS. They are accessed by clients in the following manner:

- For SMB, AFP, and HTTP/HTTPS, users are presented with a virtual share named after the username. The virtual share is visible and accessible only to the user. Users are not limited only to their virtual shares; all other shares on the server continue to be accessible in the usual fashion.
- For NFS, the home directory is exported. When a user mounts the home directory root, all home directories will be visible inside the root, but the user’s home directory will be accessible only by the user and the administrator.

  Note If desired, UNIX clients can be configured to use a Snap Home Directory as the local user’s system home directory. Configure the client to mount the home directory root for all users, and then configure each user account on the client to use the user-specific directory on the SnapServer as the user’s home directory.
- For FTP/FTPS, local users will automatically be placed in their private home directory when they log in. Access to the home directory is facilitated through a share pointing to a parent directory of the home directory, so users can still change to the top-level directory to access other shares.

If ID Mapping is enabled, domain users and local users mapped to the same user will be directed to the domain user’s home directory. In some cases, data in the local user's home directory will be copied to the domain user's home directory:

- If a local user home directory accumulates files before the local and domain users are mapped, and if the domain user's home directory is empty, the local user's files will be copied to the domain user's home directory the first time the local user connects after the users are mapped.
- If both the local and domain user home directories accumulate files before the local and domain users are mapped, the files in the local user's home directory will not be copied to the domain user's home directory.

Windows ACLs

Introduced in v5.0, GuardianOS now fully supports Windows NTFS-style file system ACLs, including configuration, enforcement, and inheritance models. Inside Windows/Mixed SnapTrees, files created and managed by Windows clients have the Windows security personality and behave just as they would on a Windows server. Clients can use the standard Windows NT, 2000, 2003, XP, Vista or Windows 7 interface to set directory and file permissions for local and Windows domain users and groups on the SnapServer.

Permissions are enforced for the specified users in the same manner for all client protocols, including non-SMB clients that normally have the UNIX security personality. However, if a non-SMB client changes permissions or ownership on a

Windows personality file or directory (or deletes and recreates it), the personality will change to UNIX with the UNIX permissions specified by the client.

Note Group membership of NFS clients is established by configuring the local client's user account or the NIS domain. Group membership of SnapServer local users or users ID-mapped to domain users is not observed by NFS clients. Therefore, ACL permissions applied to groups may not apply as expected to NFS clients.

Default File and Folder Permissions

When a file or directory is created by an SMB client, the owner of the file will be the user who created the file (except for files created by local or domain administrators, in which case the owner will be the "Administrators" group, mapped to the local admingrp), and the ACL will be inherited per the inheritance ACEs on the parent directory's ACL. The owner of a file or directory always implicitly has the ability to change permissions, regardless of the permissions established in the ACL. In addition, members of the SnapServer's local admin group, as well as members of Domain Admins (if the server is configured to belong to a domain) always implicitly have *take ownership* and *change ownership* permissions.

Setting File and Directory Access Permissions and Inheritance (Windows)

Access permissions for files and directories with the Windows security personality are set using standard Windows NT, 2000, 2003, XP, Vista, 2008, or 7 security tools. GuardianOS supports:

- All standard generic and advanced access permissions that can be assigned by Windows clients.
- All levels of inheritance that can be assigned to an ACE in a directory ACL from a Windows client.
- Automatic inheritance from parent directories, as well as the ability to disable automatic inheritance from parents.
- Special assignment and inheritance of the CREATOR OWNER, CREATOR GROUP, Users, Authenticated Users, and Administrators built-in users and groups.

To Set File and Directory Permissions and Inheritance (Windows)

1 Using a Windows NT 4.0, 2000, 2003, XP, Vista, 2008, or 7 client, map a drive to the SnapServer, logging in as a user with change permissions for the target file or directory.

2 Do one of the following:

- In Windows NT, right-click the file or directory, choose **Properties**, click the **Security** button, and then select **Permissions**.
- In Windows 2000, 2003, XP, Vista, 2008, or 7, right-click the file or directory, choose **Properties**, and then select the **Security** tab.

3 Use the Windows security tools to add or delete users and groups, to modify their permissions, and to set inheritance rules.

To View File and Directory Permissions and Inheritance (*Web View*)

1 Connect to the SnapServer *Web View:*

a In your browser, enter `http://[servername]`

b Log in as a user with admin rights on the SnapServer using the Switch User link.

Note If Web Root is enabled, log in to the administrative interface via
`http://[servername]/config`
then point your browser directly to a share to browse via
`http://[servername]/[sharename]`

2 Browse *Web View* and click on the key icon to view security configuration on files and directories.

Security Guides

Security guides are designed to assist you in setting up security for your SnapServer.

The following guides are available:

Use Windows NT Domain Security

This security guide provides steps for configuring your SnapServer to use Windows NT domain security for Microsoft Networking. Once configured, the SnapServer will accept Microsoft networking users and groups that are part of the domain. These users and groups can be granted (or restricted) access rights for SnapServer network shares, files, or directories.

The SnapServer will need the name of your Windows domain, and the name and password of an administrative user within your Windows domain.

For more information about Windows domains and other Microsoft networking settings, see “Support for Windows Networking (SMB)” on page 29 and “Support for Windows Network Authentication” on page 30.

Use Windows Active Directory Security

This security guide provides steps for configuring your SnapServer to use Windows Active Directory Security for Microsoft Networking. Once configured, the SnapServer will accept Microsoft networking users and groups that are part of the domain. These users and groups can be granted (or denied) access rights for SnapServer network shares.

The SnapServer will need the name of your Active Directory domain, the name and password of an administrative user within your Active Directory domain, and the name of the organizational unit within the Active Directory tree in which the SnapServer will appear.

For more information about Windows Active Directory, please see “Support for Windows Network Authentication” on page 30.

Share-level Access to an Entire Volume

This security guide provides steps for allowing users share-level access to a whole volume on the SnapServer. You will need to know which user to grant access to and which volume they are to access.

Share-level Access to a Folder on a Volume

This security guide provides steps for allowing users share-level access to a folder on a volume on the SnapServer. You will need to know which user to grant access to and which folder(s) they are to access.

Snapshots

A *snapshot* is a consistent, stable, point-in-time image of a volume that can be backed up independent of activity on the live volume. Snapshots can also satisfy short-term backup situations such as recovering a file deleted in error, or even restoring an entire file system, without resorting to tape. Perhaps more importantly, snapshots can be incorporated as a central component of your backup strategy to ensure that all data in every backup operation is internally consistent and that no data is overlooked or skipped.

Note The Snapshot feature described here does not apply to snapshots for iSCSI disks. Supported Windows servers can create native snapshots of iSCSI disks using VSS. For more information, see “Configuring VSS/VDS for iSCSI Disks” on page 93.

Topics in Snapshot Management:

- Snapshot Management and Usage
- Estimating Snapshot Pool Requirements
- Adjusting Snapshot Pool Size
- Accessing Snapshots
- Coordinating Snapshot and Backup Operations

Related Information:

- Isolate iSCSI Disks from Other Resources for Backup Purposes

Snapshot Management and Usage

This section describes snapshot components and dependencies.

The Snapshot Pool

Snapshot data are stored on a RAID in a *snapshot pool*, or space reserved within the RAID for this purpose. Each RAID on the system contains only one snapshot pool. This pool contains all snapshot data for all volumes on the RAID. For more information, see "Estimating Snapshot Pool Requirements" on page 113.

Rolling a Volume Back to a Previous State

If you need to restore an entire file system to a previous state, you can do so without resorting to tape. The snapshot rollback feature allows you to use any archived snapshot to restore an entire file system to a previous state simply by selecting the snapshot and clicking the **Rollback** button. During the rollback operation, data on the volume will be inaccessible to clients.

Cautions (1) Rolling back a volume cannot be undone and should only be used as a last resort after attempts to restore selected directories or files have failed; (2) Performing a rollback on a volume may invalidate the NetVault for GuardianOS NVDB directory for the volume, and may also disable the antivirus software. If you are using these features, take the necessary precautions as described in "Volumes" on page 56.

Scheduling Snapshots

Snapshots should ideally be taken when your system is idle. It is recommended that snapshots be taken before a backup is performed. For example, if your backup is scheduled at 4 a.m., schedule the snapshot to be taken at 2 a.m., thereby avoiding system activity and ensuring the snapshot is backed-up. See "Coordinating Snapshot and Backup Operations" on page 115 for more information.

Snapshots and Backup Optimization

When you back up a live volume directly, files that reference other files in the system may become out-of sync in relation to each other. The more data you have to back up, the more time is required for the backup operation, and the more likely these events are to occur. By backing up the snapshot rather than the volume itself, you greatly reduce the risk of archiving inconsistent data. For instructions, see "Coordinating Snapshot and Backup Operations" on page 115.

Snapshots and iSCSI Disks

Running a GuardianOS snapshot on a volume containing an iSCSI Disk will abruptly disconnect any clients attempting to write to the iSCSI Disk and the resulting snapshot may contain inconsistent data. Do not use GuardianOS snapshots on a volume containing an iSCSI Disk.

To create a native snapshot of an iSCSI disk on Windows systems, use the VSS feature described in "Configuring VSS/VDS for iSCSI Disks" on page 93.

Estimating Snapshot Pool Requirements

Snapshot data grow dynamically for as long as a snapshot is active and as long as there is enough space available in the snapshot pool to store them. When the snapshot pool approaches its capacity (at about 95 percent), the SnapServer deletes the oldest snapshot's data to create space for more recent snapshot data.

The default configuration allocates 80 percent of RAID capacity to the volume and 20 percent to the snapshot pool. You can adjust the size of the pool up (assuming unallocated space exists) or down according to your needs. If you find that your snapshot strategy does not require all of the space allocated to the snapshot pool by default, consider decreasing snapshot pool capacity and reallocating the capacity to the file system. To adjust the size of the snapshot pool, navigate to the **Storage > Snapshots** screen, click the **Snapshot Space** button, then click the Raid Set for the snapshot pool you want to adjust.

The number of snapshots that a RAID can support is a function of these factors:

- The space reserved for the snapshot data
- The duration of the snapshots you create
- The amount and type of write activity to the volume(s) since the snapshot was created

The following table describes minimum and maximum allocation cases.

Allocate about 10% of RAID if	Allocate about 25% of RAID if
• Activity is write-light • Write access patterns are concentrated in a few places • A small number of Snapshots must be available at any point in time	• Activity is write-heavy • Write access patterns are randomized across the volume • A large number of Snapshots must be available at any point in time

Adjusting Snapshot Pool Size

The current size of the snapshot pool for each RAID (or RAID group) can be viewed by navigating to the **Storage > Snapshots** screen and clicking the **Snapshot Space** button, then clicking the Raid Set. On the screen that opens, you can adjust the size of the pool as necessary. In addition, there are two other processes that may affect the size of the snapshot pool:

- **Creating a Volume —** In the course of creating a new volume, a pull-down menu allows you to add a percentage of the capacity being allocated to the new volume to the snapshot pool. This feature defaults to 20 percent, the recommended amount of space to reserve for snapshots. If you do not plan to use snapshots with this volume, maximize volume capacity by reducing this percentage to zero; if you do plan to use snapshots, adjust this percentage in accordance with the guidelines discussed in the previous section Estimating Snapshot Pool Requirements.
- **Creating a RAID Group —** When two RAIDS are grouped, their snapshot pools are added together. For example, if RAID A with a snapshot pool of 50 GB is grouped with RAID B with a snapshot pool of 25 GB, the resulting RAID group will have a snapshot pool of 75 GB. Depending on the purpose you had in mind when grouping the RAIDs, the result of combining the two snapshot pools may or may not be desirable, and you will need to readjust the size as described previously.

Accessing Snapshots

Snapshots are accessed via a snapshot share. Just as a share provides access to a portion of a live volume (or file system), a snapshot share provides access to the same portion of the file system on all current snapshots of the volume. The snapshot share’s path into snapshots mimics the original share’s path into the live volume.

Creating a Snapshot Share

You create a snapshot share by selecting the **Create Snapshot Share** option in the course of creating a live-volume share, under the **Advanced Share Properties** link. For example, assume you create a share to a directory called “sales,” and you select the **Create Snapshot Share** option. When you connect to the server via Internet Explorer or other file browser, two shares display:

```
SALES
SALES_SNAP
```

The first share provides access to the live volume, and the second share provides access to any archived snapshots. Other than read-write settings (snapshots are read-only), a snapshot share inherits access privileges from its associated live-volume share.

Note The same folders appear on the Web View screen when you connect to the SnapServer using a Web browser; however, the snapshot share folder does not provide access to the snapshot; it will always appear to be empty. You can prevent the snapshot share from displaying on this Web View screen by selecting the **Hide Snapshot Share** option when creating or editing a share.

Accessing Snapshots Within the Snapshot Share

A snapshot share contains a series of directories. Each directory inside the snapshot share represents a different snapshot. The directory names reflect the date and time the snapshot was created. For example, assume the snapshot share named *Sales_SNAP* contains the following four directories:

```
latest
2008-12-25.120000
2009-01-01.000100
2009-01-07.020100
```

The *latest* directory always points to the most recent snapshot (in this case, `2009-01-07.020100`, or January 7th, 2009, at 2:01 a.m.). A user may view an individual file as it existed at a previous point in time or even roll back to a previous version of the file by creating a file copy to the current live volume.

Note The latest subdirectory is very useful for setting up backup jobs as the name of the directory is always the same and always points to the latest available snapshot.

Coordinating Snapshot and Backup Operations

Like backups, snapshots can be scheduled to recur at a designated time and interval. In addition to synchronizing the backup and snapshot schedules, you must create a share (and snapshot share) to the appropriate directory so that the backup software can access the snapshot. For most backup purposes, the directory specified should be one that points to the root of the volume so that all of the volume's data is backed up and available from the snapshot share.

1 **Create a snapshot for each volume you want to back up.**

In the Administration Tool, navigate to **Storage > Snapshots,** and click **Create Snapshot**. When defining and scheduling the snapshot, consider the following:

- Put a check in the **Create Recovery File** check box to ensure that the ACL, extended attributes, and quota information are captured and appended to the snapshot. This step is needed because many backup packages do not back up native ACLs and quotas. Placing this information in a recovery file allows all backup packages to include this information. If the volume needs to be restored from tape, or the entire system needs to be recreated from scratch on a different server, this information may be required to restore all rights and quota information.

- Offset the snapshot and backup schedules such that the backup does not occur until you are sure the snapshot has been created. (The snapshot itself does not require much time, but creating the recovery file may take up to 30 minutes, depending on the number of files in the volume.) For example, assuming you schedule nightly backups for a heavily used volume at 3:00 a.m., you might schedule the snapshot of the volume to run every day at 2:30 a.m., allowing half an hour for the snapshot to run to completion.

2 **If you have not already done so, create a share for each volume with snapshot share enabled.**

In the Administration Tool, navigate to the **Security > Shares** screen, and click **Create Share**. Select the volume you want the share to point to (if you want to create a share to the root of the volume, simply accept the default path). Click **Advanced Share Properties**, then select **Create Snapshot Share**.

3 **Set the backup software to archive the latest version of the snapshot.**

The SnapServer makes it easy to configure your backup software to automatically archive the most recent snapshot. Simply configure your backup software to copy the contents of the `latest` directory within the snapshot share you created at the root of the volume. For example, assume the snapshot share named *SHARE1_SNAP* contains the following four directories:

```
latest
2008-12-25.120000
2009-01-01.000100
2009-01-07.020100
```

Each directory inside the snapshot share represents a different snapshot. The directory names reflect the date and time the snapshot was created. However, the `latest` directory always points to the latest snapshot (in this case, `2009-01-07.020100`, or January 7th, 2009, at 2:01 a.m.). In this case, configuring the backup software to copy from:

```
\SHARE1_SNAP\latest
```

ensures that the most recently created snapshot is always archived.

A rollback can disable Snap EDR and result in its removal. If this occurs, download the Snap EDR package from the SnapServer web site, reinstall it using the OS Update feature, then reenable and configure it from the SnapExtensions page.

Disaster Recovery

Disaster recovery entails creating the files you need to recover a SnapServer's configuration information, such as network and RAID configurations, as well as volume-specific information, such as ACLs and quota settings.

It also includes what to do if all access to the data on a SnapServer is cut off due to a hardware or software failure. Focus is placed on the procedures for:

- Reinstalling the SnapServer operating system
- Restoring the server to its original configuration with data intact

These files are then used to restore any SnapServer to its original state. The disaster recovery feature can also be used to clone one server to another by restoring the disaster recovery image from one server to another server.

Topics in Disaster Recovery Management:

- Backing Up Server and Volume Settings
- Backing Up the NetVault Database Directory
- Recovering the NetVault Database
- Disaster Recovery Procedural Overview
- Cloning a Server

Backing Up Server and Volume Settings

In addition to backing up the data stored on the SnapServer, you may also back up the server's system and volume settings. The **Maintenance > Disaster Recovery** screen allows you to create the files you need to restore these settings:

- Server-specific settings such as network, RAID, volume and share configurations, local user and group lists, snapshot schedules, and EDR Management Console settings (if applicable).
- Volume-specific settings such as ACLs, extended attributes, and quota settings.

The SnapDRImage File and the Volume Files

Details on the SnapServer disaster recovery files and the information they contain are as follows:

- **SnapDRImage** — The SnapServer disaster recovery image saves server-specific settings such as network, RAID, volume and share configuration, local user and group lists, and EDR Management Console settings (if applicable). There is one SnapDRImage file per server, residing on the root directory of the first volume at the following path: `\\server_name\volume_name`

  Note The SnapDRImage file is in binary form and can be safely used only with the SnapServer Disaster Recovery tool. Other tools will not work and may compromise the integrity of the file.

- **Volume-specific files —** These files, named *backup.acl*, *backup.qta.groups*, and *backup.qta.users*, preserve volume-specific settings such as ACLs, extended attributes, and quota settings. One set of these files exists per volume, residing at the following path: `\\server_name\volume_name\.os_private`

  Caution The Create Recovery Files option in the snapshot feature automatically updates the volume-specific files when the snapshot is taken. If you do not use snapshots to back up a volume to tape, you must manually regenerate these files whenever you change ACL or quota information to ensure that you are backing up the most current volume settings.

Creating the SnapDRImage and Volume Files

Creating a SnapDRImage that covers the scope of your server's configuration is essential to a successful disaster recovery operation. Create a disaster recovery image on the **Maintenance > Disaster Recovery** page. This DRImage should be created after server configuration is complete, and can be used to recover the server or a replacement server to the configured state.

Before you create the disaster recovery files, make sure you have completed the following activities:

- You have completely configured the SnapServer. If you subsequently make any major changes to the configuration of your server, you must repeat the procedures described in this section to have an up-to-date SnapDRImage.

  Note You may want to record, in an off-server location, the following information about the configuration of your server: (1) the server name; (2) the number of RAIDs; (3) the number of volumes; and (4) the size of each volume. If the disaster recovery fails, having this information may be useful in recreating the original configuration of the server.

- You have devised and implemented a data backup strategy. It is recommended that you make a backup of your system regularly, from the root of the share for each volume, and store it in an off-server location. This ensures that the most current data is backed up and available for use with a disaster recovery.

Use the following procedure to create and secure the disaster recovery files:

1 **Create the disaster recovery files.**

Navigate to the **Maintenance > Disaster Recovery** screen. Select the **Create Recovery Image** radio button and click **OK** to create the SnapDRImage file and the volume files in a single operation.

2 **Copy the files to a safe place off the server.**

Once the recovery image has been made, click the **Download Recovery Image** button to download the SnapDRImage file to a safe location on another server or backup medium. (See The SnapDRImage File and the Volume Files for file names and paths.) This strategy ensures that if the file system on the SnapServer is corrupted, the image file will be available to restore server settings.

The DRImage is also automatically placed in the root of the first user volume. These files will be copied to tape as part of your regular backup procedures.

3 **Take no action regarding the volume-specific files.**

These files will be copied to tape as part of your regular volume backup procedures.

Rejoining the Server to a Windows Domain

If you are restoring server settings to either the same physical server or to a replacement server, the server will automatically rejoin the Windows domain it was a member of before the SnapDRImage was applied as long as the servername is the same as the current servername. If you have changed the servername, you will have to manually join the server to the desired Windows domain. Navigate to **Network > Windows** to rejoin the server to a domain.

Backing Up the NetVault Database Directory

This section details the use of the NetVault Database plug-in and offers various tips for its use.

Backup Recommendations

It is important to note that the NetVault Database can be backed up at any time as long as no other NetVault jobs controlled by this server are running. With this in mind, the following points are recommended when backing up the NetVault Database:

- **Perform Regular Backups —** The data contained in the NetVault Database is integral to NetVault operations, but it also frequently changes as NetVault functions; therefore, it is recommended that frequent, regular backups of the NetVault Database be performed (e.g., daily, once all other backups have completed).
- **Target Specific Media for a NetVault Database Backup —** In the event that the NetVault Database needs to be recovered, the specific piece of media targeted can be easily located to perform the recovery.

To Back up the NVDB Directory

1. From the NetVault Server (either locally or remotely), open the NetVault Backup window by clicking the **Backup** button on the command toolbar. The NetVault Backup window displays the list of available clients in the Selections tab.
2. Right-click the NetVault Server (acting as a client to itself) and select **Open** from the pop-up menu.
3. The available plug-ins will be displayed. Right-click the NetVault Database Plug-in and select **Open** from the pop-up menu that appears.
4. A single selectable item will be revealed: the NetVault Database. Select the check box to the left of this item.

   Note There are no Backup Options available for use with this plug-in.
5. The remaining tab selections (Schedule, Target Advanced Options) contain additional options that can be set as desired.
6. Enter a suitable name for the job in the Job Title box and start the backup job by clicking the **Submit** button on the command toolbar.

   Note Only clients successfully added via the NetVault Client Management window will display.

Recovering the NetVault Database

This section summarizes the procedure necessary for recovering the NetVault Database (NVDB) from tape. For instructional details, see the NetVault documentation that shipped with your SnapServer.

Pre-Restore Requirements

Before restoring the database, perform the following steps on the SnapServer acting as the NetVault Server:

1. Completely reinstall and configure the same version of the GuardianOS that the server was running. The OS installation will also reinstall the NetVault Server software.
2. If necessary, navigate to the **SnapExtensions** screen and re-enable the NetVault software.
3. Remove all media from the device(s) used by the NetVault Server, except the media that contains the backup saveset needed for the recovery of the NVDB.
4. Add all devices previously added to the NetVault Server through the use of the Device Management window.
5. From the Device Management window, the media containing the backup saveset will be recognized as FOREIGN in its designated drive or library slot. Scan the media before proceeding with the restore operation.

Restore Recommendations

The following recommendations are offered for the process of recovering the NVDB:

- **Perform a Full Recovery of the NetVault Database —** Although NetVault offers provisions for recovering individual elements of the NVDB, it is recommended that a full recovery be performed. If recovering individual components, it is strongly recommended that this be performed under the guidance of BakBone Technical Support.
- **Do Not Monitor Job Progress During a Recovery —** It is strongly recommended that all NetVault windows be closed, and the NetVault GUI be closed during the recovery of the NVDB, as this may interfere with the process.

Restore Procedure

1. Access the Restore window from the NetVault GUI by clicking the **Restore** button in the command toolbar.
2. Double-click the **NetVault Server** that the desired backup was performed from to open it.
3. Plug-ins (and APMs) used to conduct successful backups on the selected client will be displayed. Double-click the **NVDB Plug-in** to open it.
4. All of the backup savesets are created using the NVDB Plug-in display. Locate the desired saveset, right-click it and select **Open** from the pop-up menu.
5. All of the various components that make up the NVDB will display. Items with check boxes at their left are single items that can be selected for inclusion, while items without check boxes can be double-clicked to browse their individual contents.
6. For a full database restore, select each item in the tree. Additionally, open up root items to display their contents by double-clicking them, and then select all of their contents (e.g., Events, Notification and Reports Database items).
7. Select the **Restore Options** tab and make sure that the Blank Reports Database Table option is selected.
8. Other tab selections (e.g., Schedule and Advanced Options) contain additional options that can be set as desired.
9. Enter a suitable name for the job in the Job Title box and start the restore job by clicking the **Submit** button.
10. The job will now run and the backed-up version of the NVDB will be restored over the one created with the recent installation of NetVault.
11. Once the NVDB has restored successfully, it is necessary to restart NetVault Services via the NetVault Configurator. During the restore procedure these services are automatically stopped.

Disaster Recovery Procedural Overview

The procedure described in this section for responding to a catastrophic event is general in nature and may result in the loss of data. Should such an event actually occur, the exact procedure to follow will vary according to environmental conditions. Overland Storage strongly recommends that you contact a technical service representative before proceeding.

This section describes a worst-case scenario:

- The operating system has failed, (e.g., due to a malicious attack to the root file system), and you cannot access the server.
- The data has been corrupted and must be restored from tape.
- Technical support has deemed your server unsalvagable and provided you with a new, unconfigured server.

Restoring Previous Server Settings to a New Server

After Technical Support has supplied you with a new server, you can restore the settings from the previous server to the new server. Any third-party license keys you have not purchased through Overland Storage will be lost. If you have installed data replication or management utilities such as Snap EDR, you will need to re-install and/or relicense them for use with the new server.

Note If you are restoring EDR Management Console settings, you must recreate the RAID and volume configuration that matches the DRI settings, then install and enable the EDR Management Console. As an alternative, you can first restore just the system settings, install EDR, and then restore just the EDR settings.

You will also need to reschedule snapshots as well reconfigure CA Antivirus.

Note If you are restoring the DRImage to the same server, all your license keys should be intact. You will still need to reschedule your snapshots and CA Antivirus.

1. When you connect to the new server, navigate to **Maintenance > Disaster Recovery**, select **Recover System Settings** and click **OK**.
2. Click the **Browse** button and navigate to the Snap DRImage you made of the previous server, then click **OK**.
3. The server will reboot and the settings will be restored. To view the log, click the date link on the Disaster Recovery screen after the server has rebooted.
4. After restoring your server settings, rejoin the server to the Windows domain if necessary.

5 Now you can replace your data from tape backup. If the backup doesn’t retain permission and ownership settings, you can restore these by selecting **Recover Volume Security Settings** on the **Maintenance > Disaster Recovery** screen.

Note If you are restoring from any backup other than NetVault, you will need to recover the volume settings.

Cloning a Server

The Disaster Recovery process can be used to clone a server in order to apply the same configuration to one or more servers. To clone a server:

1 Create a disaster recovery image on the source server (refer to Creating the SnapDRImage and Volume Files).

2 Copy the disaster recovery files from the source server to a client.

3 Perform a disaster recovery restore procedure to each of the clone target servers using the disaster recovery files from the source server (refer to Restoring Previous Server Settings to a New Server).

CA *e*Trust Antivirus Software

The CA *e*Trust Antivirus software is preinstalled on all GuardianOS SnapServers. By default, the software is enabled on most SnapServers, but no scan jobs or signature updates have been scheduled. (The server will, however, check for signature updates whenever the server boots.) These and other antivirus configuration and management tasks are performed using the CA *e*Trust Antivirus GUI, accessed from the **SnapExtensions > CA Antivirus** screen of the Administration Tool. This section outlines the major steps in configuring the antivirus software. See the GUI online help for detailed descriptions of all options.

Note Some SnapServers require a license before CA *e*Trust Antivirus can be enabled.

Topics in Antivirus Configuration:

- Antivirus Dependencies
- Launching the CA eTrust Antivirus GUI
- The Local Scanner View
- Scan Job Configuration and Scheduling
- Signature Updates
- Alert Options
- The Move Directory
- Log View

Note Antivirus functions or options not relevant to the SnapServer have been disabled in the configuration GUI.

Antivirus Dependencies

The SnapServer implementation of CA *e*Trust Antivirus software includes the following features:

HTTP Access and Antivirus Configuration

To access the CA *e*Trust Antivirus configuration interface, HTTP must be enabled on the **Network > Web** screen.

Re-enabling the Antivirus Software

The antivirus software is enabled by default. If the antivirus software is reinstalled (as part of an upgrade process, for example), you will need to enable the software by going to the SnapExtensions screen and clicking **CA Antivirus**. On the CA Antivirus screen, click the check box next to **Enable**, then click **OK**. If you want to reconfigure the antivirus software (rather than using the defaults), click the **Configure eTrust Antivirus** link.

Resetting the Server Date and Time

If the current server date and time are changed to an earlier date and time (**Server > Date/Time**), the change does not automatically propagate to any scheduled antivirus operations. To synchronize scheduled antivirus operations with the new date and time settings, you must reschedule each operation.

New jobs may be affected by the time change. Be sure to check that new jobs have been executed if a date or time change has been made to the server.

Storage Configuration and the Antivirus Software

The antivirus software resides on the largest volume (that existed at the time the software was installed). If you delete this volume, the CA *e*Trust Antivirus software will also be deleted. The SnapServer automatically reinstalls the antivirus software on the largest remaining volume on the system.

Note The antivirus reinstallation process does not preserve custom antivirus configuration settings. Make a note of any such settings before deleting a volume.

Launching the CA eTrust Antivirus GUI

The CA *e*Trust Antivirus software is enabled by default. Some situations, such as deleting a volume or performing an upgrade procedure, may require you to re-enable the software. To learn how the antivirus software interacts with other GuardianOS software components, see "Antivirus Dependencies" on page 126.

Launching the CA eTrust Antivirus Browser Interface

The first time you connect to the GUI, it may take from 30 seconds to several minutes for the application to load, depending on the speed of your connection.

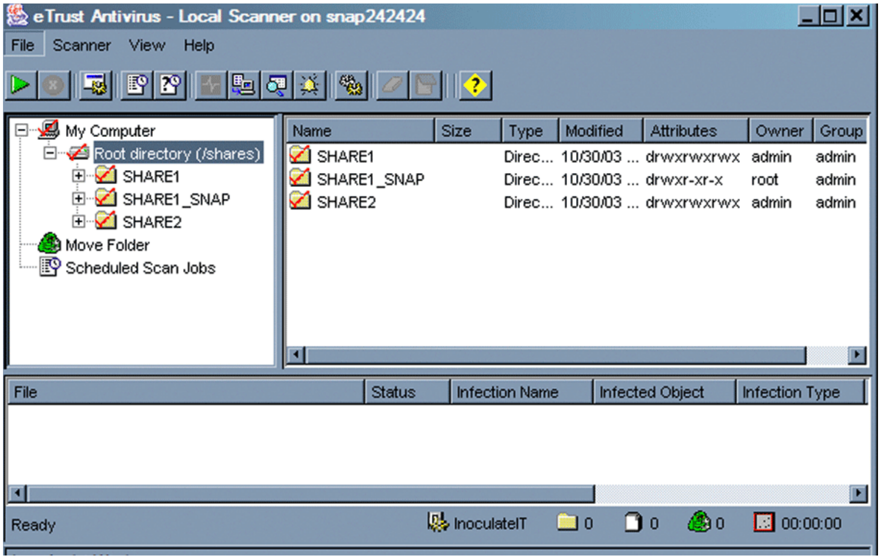
1 If you need to enable the antivirus software, go to **SnapExtensions > CA Antivirus**, click the check box next to **Enable,** and click **OK.**

2 Click the **Configure *e*Trust Antivirus** link. The splash screen opens first, followed momentarily by the GUI login dialog box.

3 Enter the same administrative user name and password (case sensitive) you have established for the Administration Tool, and then click **Login**. The antivirus GUI box opens.

The Local Scanner View

Use the Local Scanner view to scan a SnapServer for infected drives, folders, files, or disks on demand.



Name	Size	Type	Modified	Attributes	Owner	Group
SHARE1		Direc...	10/30/03 ...	drwxrwxrwx	admin	admin
SHARE1_SNAP		Direc...	10/30/03 ...	drwxr-xr-x	root	admin
SHARE2		Direc...	10/30/03 ...	drwxrwxrwx	admin	admin

File	Status	Infection Name	Infected Object	Infection Type

Component	Description
Root Directory	Displays the directory structure of the SnapServer. As in Windows Explorer, click folder icons to navigate the structure and display subfolders and files in the right-hand pane.
Move Folder	May contain infected files. The administrator can instruct the software to automatically move infected files to this directory. For more information, see “Scan Job Configuration and Scheduling” on page 128.
Scheduled Scan Jobs	Scan Jobs you schedule appear in this folder. For more information, see “Scheduling a Scan Job” on page 130.

Scan Job Configuration and Scheduling

You can run scan jobs on demand or you can configure scan jobs to run periodically. This section outlines the process of configuring and running manual and scheduled scans. For detailed descriptions of all scanning options, see the CA *e*Trust Antivirus online help.

Note You may not want to include Snapshot shares (see “Snapshot Management and Usage” on page 112) as part of your virus scan. Because access to an archived version of the file system provided by a snapshot share is read-only, you cannot treat or move any infected file; you would have to delete the entire snapshot to effect a cure. A more useful approach is to always scan your file system for viruses before running a snapshot. Adjust your antivirus scan schedule to synchronize with your snapshot schedule so that any infected files are cured or removed before the snapshot is scheduled to fire.

Defining Scan Jobs

This section provides an overview of the major choices available in configuring scan jobs. Access these options by selecting **Local Scanner Options** from the Scanner Menu.

Choosing an Infection Treatment (Scan Tab)

You can instruct the software to perform one of the following file actions when an infected file is found:

File Actions	Description
Report Only	(Default) Reports when an infection is found.
Delete File	Deletes an infected file.
Rename File	Renames an infected file with an AVB extension. Infected files with the same name are given incremental extensions (e.g., FILE.0.AVB, FILE.1.AVB, and so on). After a file is renamed with an AVB-type of extension, it is not scanned subsequently.
Move File	Moves an infected file from its current directory to the Move directory for quarantine.
Cure File	Attempts to cure an infected file automatically. Choosing this setting enables the **File Options** button. Click this button to display the Cure Action Options and specify how the Cure File option performs. **Note** The *System Cure* option is not available on SnapServers.

Setting the Type of Files to Scan (Selections tab)

Use the Selections tab options to choose the types of objects to scan, the types of file extensions to include or exclude from a scan, and the types of compressed files to scan.

- **File Extensions —** You can choose to scan files regardless of extension, or select specific types of extensions to include or exclude.
- **Compressed Files —** To scan compressed files, select the *Scan Compressed Files* check box, and then click **Choose Type** to specify the compressed file extension types.

Filtering File Information for Logs (Manual Scans Only)

You can specify the types of events that are written to a log. Check the *Infected files* option to put information in the log about files that are found to be infected. Check the *Clean files* option to put information in the log about files that are scanned and are not infected. Check the *Skipped files* option to put information in the log about files that have been excluded from the scan.

Running a Manual Scan Job

Before running a local scan job, confirm that the scanner options are correctly configured as described in the previous section.

1 **In Local Scanner View, select the folders you want to scan.**

The left-hand pane displays the directory structure of the SnapServer. A red check mark on a folder or file indicates that it is selected for scanning. (By default, all directories and files are selected for scanning.) Click folders or files to toggle file/folder selection on or off.

2 **Run the scan.**

Select **Scanner > Start Scanning**. The interface is unavailable for further configuration while the scan is in progress. The scan results display in the lower pane of the Local Scanner View, and the action taken with each file is listed in the Status column.

Scheduling a Scan Job

A scan job is configured and scheduled in the Schedule New Scan Job dialog box. To open this dialog box, select the **Scanner > Schedule Scan Job > Create** command.

1 **Set scan options in the Scan and Selection tabs.**

These options are summarized in “Defining Scan Jobs” on page 128.

2 **Schedule the scan.**

The Schedule tab allows you to set a start date and a repeat interval for the scan.

3 **Select the directories to scan.**

The Directories tab lists all paths that currently exist on the server. You can remove or add new paths as desired. You can also use the Exclude Directories tab to achieve the same result.

4 **Click OK.**

You can view scheduled scan jobs by clicking the **Scheduled Scan Jobs** folder in the Local Scanner View. To edit a job, right-click it and select **Options**.

Signature Updates

Signature updates contain the latest versions of the signature files that recognize the latest infections. They also contain the latest engine versions, which do the work of looking for infections. Signature updates are made available on a regular basis by Computer Associates.

These updates are cumulative, so they contain everything from all previous file updates, plus the newest information on the latest infections. If you have missed a recent update, you only need to collect the latest signature file to have the most up-to-date protection.

SnapServers are preconfigured to download signature updates from the CA FTP site at ftp://ftpav.ca.com/pub/inoculan/scaneng. By default, no signature updates are scheduled. The antivirus software will, however, check for signature updates whenever the server is powered on. To update SnapServers that do not have Internet access, the following methods are available:

Method	Description
FTP	Use FTP to download the update files from the Computer Associates FTP site. You can also use FTP to distribute signature updates from one SnapServer (or any FTP server) to another. **Note** When using FTP, the user name and password are passed as clear text.
UNC	Use UNC to distribute signature updates from one SnapServer to another (or from any arbitrary SMB or Windows server). Note that for UNC to work, you must have the Enable Guest Account option enabled (**Network > Windows**) on the SnapServer on which the signature updates reside. **Note** Alternatively, you can distribute updates to SnapServers from any Windows/SMB server. If using this method, make sure the guest account on the chosen server exists, is enabled, and has a blank password.
Local Path	As part of the procedure to provide signature updates to the SnapServer with no Internet access, you can connect to a local path relative to the root (e.g., /shares/SHARE1/virusdefs). Note that the path to the share is case sensitive.

Updating SnapServers that have Internet Access

If your SnapServers have direct access to the Internet, you only need to schedule the downloads to set up automatic signature updates. If access to the Internet is routed through a proxy server, you may also need to specify the name of the proxy server. Both procedures are explained below:

To Schedule Signature Update Downloads

1. Choose **Scanner > Signature Update Options**.
2. On the Schedule tab, click **Enable Scheduled Download**. Select the initial download date and time, then select how often to repeat the download.
3. Click **OK**.

To Specify a Proxy Server

1. Navigate to **Scanner > Signature Update Options**, and click the **Incoming** tab.
2. Select *FTP* in the list box, then click **Edit**.
3. In the Proxy Name field, enter the IP address of the proxy server, then click **OK**.

Updating a SnapServer that does not have Internet Access

If you have SnapServers that do not have Internet access, use the following procedures to download the signature files to a machine with Internet access and then copy them to the SnapServer.

Note When retrieving signature updates, the antivirus software attempts to connect to all the sites in the site list in the order they are listed. To avoid delays or superfluous error messages, delete the default FTP option from the list on SnapServers that have no Internet access.

1. Using a workstation with Internet access, go to ftp://ftpav.ca.com/pub/inoculan/scaneng and download the following files.
   - All **.tar* files containing the word *Linux*, e.g., *fi_Linux_i386.tar* and *ii_Linux_i386.tar*
   - All **.txt* files containing the string *Sig*, e.g., *Siglist.txt* and *Siglist2.txt*
2. Using a method appropriate to your environment, copy the update files to the SnapServer.
3. Navigate to **Scanner > Signature Update Options**, and click the **Incoming** tab.
4. Click the **Add** button, then select *Local Path* from the Method pull-down menu.

5 In the Path field, enter the path to the directory on the server on which the update file resides. If you are using a SnapServer, the path would be similar to the following:

/shares/*SHARE1/sigfiles*

where *SHARE1/sigfiles* is the share path to the directory containing the signature update files.

6 Click **OK**. The path appears in the list box.

7 Click **Download Now**.

Distributing Updates from One Server to Another

When retrieving signature updates, the antivirus software attempts to connect to all the sites in the site list in the order they are listed. To avoid delays or superfluous error messages, delete the default FTP option from the list on SnapServers that have no Internet access.

To Distribute Files via UNC

If you have more than one SnapServer with no Internet access, you can perform the previous procedure on just one of them (or any Windows/SMB server), and then configure your other SnapServers to get the update from that server automatically via SMB by specifying the UNC of the server containing the signature files.

Notes The following conditions must be met in order to distribute updates using UNC:

- The correct Signature files must have been downloaded to the root of the share being used for updates.
- The server containing the Signature updates must have the Guest account enabled (**Network > Windows**) in GuardianOS. For other SMB/CIFS servers, the Guest account must have no password, and there may be additional requirements (e.g., Windows servers must allow anonymous connections).
- The share and Signature files must be accessible to the Guest account.
- The server name used in the UNC must be resolvable by the server running CA Antivirus.

1 Navigate to **Scanner > Signature Update Options**, and click the **Incoming** tab.

2 Click the **Add** button, and select **UNC** in the Method list box.

3 Enter the path to the SnapServer (or Windows/SMB server) to which the update files have been downloaded (see previous procedure) using the following format:

```
\\server_name\share_name
```

where *server_name* is the name of the server, and *share_name* is the name of the share providing access to the files. (On a SnapServer, the update files must reside on the root of the share.)

4 Click **OK**. The path you entered appears in the Download Sources list box.

5 Click **Download Now**.

To Distribute Files via FTP

If you have more than one SnapServer with no Internet access, you can perform the FTP download procedure on just one of them (or any FTP server), and then configure your other SnapServers to get the signature updates from that server automatically via FTP.

1 Navigate to **Scanner > Signature Update Options**, and click the **Incoming** tab.

2 Click the **Add** button, and select **FTP** in the Method list box.

3 Enter the following information regarding the server on which the update file resides as follows:

- In the Host Name field, enter the IP address.
- In the User Name and Password fields, enter the admin user name and password.
- In the Remote Path field, enter the path to the directory in which the file resides. If you are using a SnapServer, the path would be similar to the following:

  /shares/*SHARE1/sigfiles*

  where *SHARE1/sigfiles* is the share path to the directory containing the signature update files.

4 Click **OK**. The path you entered appears in the Download Sources list box.

5 Click **Download Now**.

Verifying Download Events

Use the following procedure to verify download and distribution events.

1 Select **View > Log Viewer**.

2 In the left-hand pane, select **Distribution Events**. Distribution events are listed in the upper right-hand pane in chronological order.

3 Select a distribution event. The details of the distribution event display in the lower pane.

Alert Options

Alert options allow you to tailor the notification information that is provided to the Alert Manager, cut down on message traffic, and minimize the dissemination of notifications that are not critical. To set alert options, select **Alert Options** from the Scanner menu. The Alert Options dialog box contains the following tabs:

Tab	Description
Report	Use the Alert Report options to specify where to send notification information, and the Report Criteria options to manage how frequently messages from the General Event Log are reported. **Note** The Local Alert Manager option is not supported on SnapServers.
Alert Filter	Use the Alert Filter options to manage notification severity levels, and to determine what types of messages should be passed to the Alert Manager. **Note** In the Custom Notification Module, the *Realtime Server* and *Admin server* settings have no effect on SnapServers.

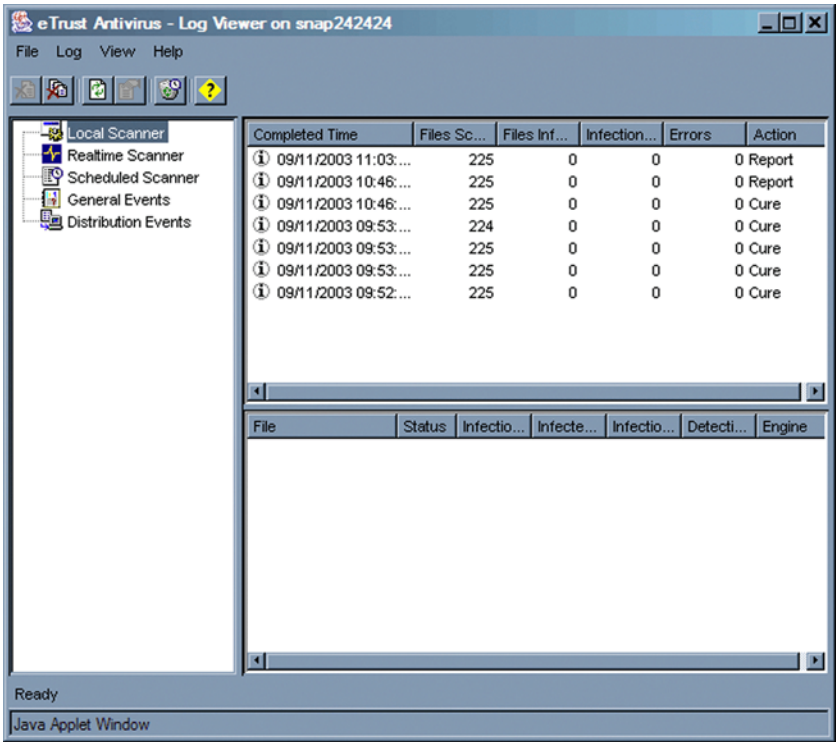
The Move Directory

You can configure scans to move infected files to the move folder (**Scanner > Local Scanner** options). To view infected files, click the **Move** directory on the left-hand pane of the Local Scanner View. To manage a moved file, right-click the file and select from the following options:

Option	Description
Restore	This option removes the file from the Move Folder and restores it to its original location with its original name and type.
Restore as	This option displays a dialog box that allows you to change the directory location and file name. You can rename a file and isolate it safely in a different location. You may want to use this option, for example, if you do not have another source for the data and you need to look at the file. Or you may have a file that you want to analyze. **Note** To restore a file to a different directory, you must prepend the path to the directory with the string /shares. For example, to restore a file to the SHARE1/sales directory, enter the path as follows: /shares/SHARE1/sales
Restore and Cure	This option allows you to restore the selected item back to the original folder it was in, and cure it. This option is useful if you update the signature files after items have been put in the Move folder. If a cure is provided that you did not have available, you can get the latest signature update and use this option to restore and cure an infected item.
Delete	This option deletes the infected file; no warning or confirmation message is displayed.

Log View

The Log View provides easy access to detailed information on scan, distribution, and other events. To access this view select **Log View** from the View menu.



Completed Time	Files Sc...	Files Inf...	Infection...	Errors	Action
ⓘ 09/11/2003 11:03:...	225	0	0	0	Report
ⓘ 09/11/2003 10:46:...	225	0	0	0	Report
ⓘ 09/11/2003 10:46:...	225	0	0	0	Cure
ⓘ 09/11/2003 09:53:...	224	0	0	0	Cure
ⓘ 09/11/2003 09:53:...	225	0	0	0	Cure
ⓘ 09/11/2003 09:53:...	225	0	0	0	Cure
ⓘ 09/11/2003 09:52:...	225	0	0	0	Cure

Option	Description
Local Scanner	Displays summary information about scan jobs that have run.
RealTime Scanner	Not Supported.
Scheduled Scanner	Displays summary information on scheduled scans that have run.
General Events	Displays the Event log for a given day. Click a date to view all events that occurred that day.
Distribution Events	Displays distribution events by date. Click a date to view detailed information on the distribution event in the lower pane.

Unicode

This section details how the GuardianOS SnapServer operates when Unicode is enabled.

Topics in Unicode

- What is Unicode?
- Converting to Unicode
- Unicode and Protocol Interaction
- How Snapshots Interact with Unicode
- Backing Up Unicode Servers
- Unicode and Expansion Arrays

What is Unicode?

GuardianOS supports Unicode. Unicode defines a universal means of representing characters in all languages. In the case of SnapServers, this allows better interoperation of varying languages using different alphabets and character sets in file and user names. More information is available at http://www.unicode.org.

Caution Once Unicode has been enabled on a GuardianOS SnapServer, it is not possible to disable Unicode. Enabling Unicode will alter the functionality of some third party applications and SnapExtensions that do not fully support Unicode.

Converting to Unicode

To convert your GuardianOS SnapServer to Unicode, complete the following steps:

Step 1: Make a DRImage of your current system and volume settings

Before converting your system to Unicode, configure all system and volume settings, then make a DRImage of your system and volume(s). This is to ensure all your settings and data are saved should something unforeseen happen during the Unicode conversion process. For more information about creating a DRImage, please see “Disaster Recovery Procedural Overview” on page 123.

Step 2: Back up your system

Back up your system as you normally would. For more information about backing up your server, please see “Backing Up Server and Volume Settings” on page 117.

Step 3: Convert to Unicode

Navigate to **Server > Unicode** and enable Unicode. Once it has been enabled on your SnapServer you cannot disable Unicode. Be sure your settings and data have been saved to an off-server location before enabling Unicode.

If NFS is enabled on your system, you must also select a client code page that will be used by NFS clients. Options include ISO-8859-1, ISO-8859-15, EUC-JP, and UTF8.

Caution Do not convert to Unicode if your volume is full. Unicode requires space on the volume for a reference file. If the volume is full, Unicode will not convert the system properly and might cause data corruption.

Once you have converted to Unicode, it is important to note the following:

- The server reboots after Unicode has been enabled.
- After rebooting, the server will convert all file systems to Unicode file names, which can take some time.
- File systems **are** accessible during conversion. During this time, file names with extended characters in them before Unicode was enabled will appear with garbled characters before being converted to Unicode.
- File system conversion is made assuming code page 1252. If files with extended characters were written to the server via NFS or FTP prior to Unicode conversion, and the NFS or FTP client was operating in a code page other than 1252 or ISO 8859-1, these characters may not convert properly.
- A small number of extended characters (about 10 total characters) written by Macintosh clients over AFP will be converted with different characters than originally written.
- Prior to Unicode conversion, if Macintosh clients are connected to the server selecting a code page other than MacRoman (US), extended characters written by those clients may not convert properly.
- Local users are converted to Unicode assuming the original source is code page 1252.

Step 4: Make a new DRImage

Once your system has been converted to unicode, make a new DRImage. The procedures are the same as before (see “Disaster Recovery Procedural Overview” on page 123 for more details).

Step 5: Back up the system with Unicode enabled backup applications

Back up your system with a Unicode compliant backup application. Please see the following section “Backing Up Unicode Servers” on page 143 for more information.

Unicode and Protocol Interaction

Extended characters in filenames are encoded on the SnapServer file system using UTF8, a method of representing all Unicode characters. However, network protocols and clients vary in their support of Unicode and UTF8, which has ramifications in the way they interact with one another when sharing files with extended characters in filenames.

The following sections describe how different protocols interact with extended characters.

SMB

Most Windows and MacOS X clients, as well as the SMB protocol, support the majority of Unicode characters. Therefore, in general, all characters written by Windows and MacOS X clients will be properly retained and visible to other Windows and MacOS X clients and Unicode-compliant protocols.

However, if there are characters on the file system that are invalid UTF8 or are otherwise not mappable to the Unicode encoding method (UCS2) used by the SMB protocol, an escape sequence will display in the file name of the file being read. Escape sequences begin with **{!^.** The following two characters are the hexidecimal value of the characters in the filename; for example, you might see **{!^AB** in a file name. Windows and MacOS X clients can edit such files, and the names will be retained in their original form when written back to the file system.

AFP

MacOSX and higher use the same method to represent Unicode characters as the SnapServer: UTF8. Information written to the server from MacOSX or higher will be encoded wth UTF8 and should be viewed correctly from the MacOS UI. However, similarly to SMB clients, characters in filenames that are incompatible with UTF8 will be returned with an escape sequence. Escape sequences begin with **{!^.** The following two characters are the hexidecimal value of the characters in the filename;

for example, you might see **{!^AB** in a file name. MacOSX clients can edit such files, and the names will be retained in their original form when written back to the file system.

MacOS 9 and lower are not Unicode-compliant, and use the MacRoman code page to represent extended characters. AFP translates MacRoman into UTF8 when writing to SnapServers. Any extended characters on the file system that cannot be translated to MacRoman will also be returned with an escape sequence.

NFS

The NFS protocol is not Unicode-compliant or -aware. Addtionally, there is no means for the SnapServer to determine what method is being used by the client to represent extended characters. Currently, the code pages most commonly used in Linux environments are: 8859-1, 8859-15, and EUC-JP. The SnapServer then must make an assumption to enable it to translate to and from UTF8 on the file system. Therefore, when in Unicode mode, you must configure the SnapServer's NFS protocol for the code page being used by NFS clients. Code page options include ISO-8859-1, ISO-8859-15, EUC-JP, and UTF8.

Any extended characters on the file system that cannot be translated to the configured NFS code page will be returned to the NFS client with an escape sequence. Escape sequences begin with **{!^.** The following two characters are the hexidecimal value of the characters in the filename; for example, you might see **{!^AB** in a file name.

FTP

FTP only supports ASCII characters by specification. Some clients bend the specification to allow extended characters, but there is no standard means of representing them. Therefore, no translation is performed on extended characters for FTP clients — all filenames are written to and read from the file system as a "bag-of-bytes". This has two ramifications: extended characters written to the file system by other protocols will be visible to FTP clients as garbled characters; and FTP clients are able to write invalid UTF8 characters to the file system. For the latter case, when other protocols encounter invalid UTF8 characters on the file system (which normally can only be written by FTP), the characters will be returned in an escape sequence. Escape sequences begin with **{!^.** The following two characters are the hexidecimal value of the characters in the filename; for example, you might see **{!^AB** in a file name.

HTTP

HTTP integrates easily with Unicode and the SnapServer. If invalid UTF8 characters are encountered on the file system, the characters will be returned with an escape sequence. Escape sequences begin with **{!^.** The following two characters are the hexidecimal value of the characters in the file name; for example, you might see **{!^AB** in a file name.

CA Antivirus

CA Antivirus is not Unicode-aware. While the CA Antivirus UI displays garbled characters for extended characters when Unicode has been enabled, it can still scan files, find viruses, clean viruses, move, and rename virus-infected files.

How Snapshots Interact with Unicode

Snapshots taken before the SnapServer was converted to Unicode are not compatable with the SnapServer once it has become Unicode enabled. It is not recommended that a pre-Unicode snapshot be used to restore a post-Unicode server.

Note It is recommended, if you have snapshots on your server from pre-Unicode conversion, you delete all snapshots once the server has been converted to Unicode.

Backing Up Unicode Servers

Backing up a Unicode-enabled SnapServer requires you to use specific methods depending on the type of client you have in use. It is recommended that like languages be used across the backup process. For example: Russian files on a localized Russian server should be backed up with a Unicode-compliant/Russian localized backup application. Mixing languages between applications can result in data corruption.

The following table gives an overview of how Unicode interacts with backup applications:

	Bakbone NetVault over client[1]	Symantec Backup Exec 10.d, 11.d, 12.d over SMB only	Symantec NetBackup 6.5	CA ARCServe 11.5, 12.0 over SMB only[1]	EMC Legato Networker v7.3, 7.4 over SMB only	Snap EDR over Sync only
Officially Supports Unicode	no	no	no	no	no	no
UI Displays Correct Filenames	no	yes	no	no	no	no
Backups and Restores Unicode data	yes	yes	yes	yes		yes

[1] The UI displays garbage but the data is intact.

Backing Up Using Unicode-Enabled Windows Clients

When backing up using a Unicode-enabled Windows client, connect and backup using SMB. It is recommended that you use Symantec Backup Exec to backup via Unicode-enabled Windows clients, but any Unicode-compliant Backup application should also work.

Backing Up Using Unicode-Enabled UNIX Clients

Most Unicode-enabled UNIX clients run one of three language codes: 8859-1 (US), 8859-15 (Europe), or EUC-JP (Japan). In each of these situations, it is important to backup via the UNIX client with a language compliant backup application. Mixing languages (example: having a Japanese UNIX server and a Chinese backup application) will lead to data corruption. If you do not have language compliant backup applications, do not back up using UNIX.

Backing Up Using Unicode-Enabled MacOS Clients

Macintosh text encoding UTF8 is supported by MacOS 10.1.4 AFP 3 and later. For Unicode to function properly, your version of MacOS must fully support AFP 3.

It is important to back up via the MacOS client with a language compliant backup application. Mixing languages (example: having Russian files on a server, then using a German backup application) will lead to data corruption.

Unicode and Expansion Arrays

This section outlines how SnapServer expansion arrays interact with Unicode.

Unicode Converted Expansion Arrays

When an expansion array is converted to Unicode, it stays converted to Unicode. This means that a Unicode enabled expansion array is only compatable with head units that have also been converted to Unicode.

The following is a usage scenario concerning expansion arrays and how they operate with Unicode enabled servers.

You have a SnapServer and an expansion array. You enable Unicode on both. You cannot then attach the expansion array to a non-Unicode-enabled SnapServer. The Unicode-enabled expansion unit will not be seen by a non-Unicode enabled server.

Once an expansion array has been converted to Unicode, it cannot be used with non-Unicode enabled SnapServers.

Unicode Converted Head Units

When a SnapServer is converted to Unicode, it stays converted to Unicode. If a non-Unicode expansion array is attached to a Unicode-converted SnapServer, the expansion array will be automatically converted to Unicode when it is incorporated with the SnapServer.

Caution Converting to Unicode is a one-way operation. There is no undoing the conversion to Unicode if you change your mind.

Backup and Replication Solutions

GuardianOS supports several backup methods, including third-party off-the-shelf backup applications and applications that have been customized and integrated with the GuardianOS on the SnapServer.

Note Enabling Unicode on the server will limit some backup applications' ability to function with the SnapServer. Refer to "Unicode" on page 139 for more information.

SnapServer Backup		Backup and Replication Solutions					
		BakBone NetVault for GuardianOS	Snap EDR	CA BrightStor ARCserve 11.5, 12.0	EMC Legato NetWorker v7.3, 7.4	Symantec Backup Exec 11.d, 12, 12.5	Symantec NetBackup 6.5
GuardianOS	Snap to Backup Server via installed agent	X[1]		X	X	X	X
	Snap to Backup Server via network protocol			X		X	
	SnapServer(s) to SCSI-attached tape drive[2] (disk-to-tape backup)	X					
	SnapServer(s) to USB-attached tape drive (disk-to-tape backup)	X					
	Backs Up Security Meta Data	X	X				

[1] The NetVault agent is preinstalled on SnapServers running GuardianOS v3.0 or higher.
[2] The tape drive/library is attached to one of the SnapServers (not applicable to the SnapServers 110 and 210).

This appendix provides a brief description of the supported backup solutions and, where applicable, gives instructions on how to install the solutions on the SnapServer.

Integrated Backup Solutions for the SnapServer

The following backup solutions are preinstalled and/or customized for the SnapServer:

BakBone Netvault

BakBone Netvault is a scalable, enterprise-wide backup solution for GuardianOS, Windows, Linux, and UNIX operating systems with the following functionality:

- **Near-line storage** — The SnapServer manages backup jobs, locally storing the backup images on disk using virtual tape library technology. Eight virtual drives with up to 100 GB capacity (total) are supported. (Additional capacity up to 1.1 TB can be added with additional licenses.)
- **Direct-attached storage** — Data from up to five clients is backed up to a standalone, SCSI-attached tape device attached to a SnapServer. Supports up to four tape drives.

Some SnapServers ship with BakBone's NetVault server software preinstalled with a Workgroup Server license. This license supports backup and recovery of data to the SnapServer from up to 5 heterogeneous clients. (Additional clients can be added with optional licenses.)

Note SnapServers 110, 210, and N2000 require an additional license to support NetVault.

For additional information on installing and configuring NetVault, see the documentation included with the NetVault CD that shipped with your SnapServer.

To Enable NetVault for GuardianOS

To enable NetVault, click the **Bakbone Netvault** link on the SnapExtensions page, check the **Enable** box, and click **OK**.

Adding Clients to the NetVault Management GUI

The **Add Clients** button allows you to specify the name or IP address of the workstation on which the NetVault management GUI has been installed.

1. Click **Add Clients** on the BakBone NetVault page.
2. Enter the management workstation's DNS name or IP address.
3. Enter the NetVault client password created during installation for the client. The password field cannot be left blank.
4. Click **Add**.

You can add multiple workstations by completing the fields and repeatedly selecting the **Add** button. This should only be done when management of your NetVault implementation MUST be managed from more than one workstation. Each client added in this way consumes a NetVault node license. Other NetVault Clients can be added using the NetVault Management GUI.

Snap Enterprise Data Replicator (Snap EDR)

Snap EDR provides server-to-server synchronization by moving, copying, or replicating the contents of a share from one SnapServer to another share on one or more different SnapServers. It comes preinstalled on some servers with a 45-day free trial, or it can be downloaded from the SnapServer website.

Snap EDR consists of a Management Console and a collection of Agents. The Management Console is installed on a central system. It coordinates and logs the following data transfer activities carried out by the distributed Agents:

- Replicates files between any two systems including Windows, Linux, and Mac Agents.
- Transfers files from one source host to one or more target hosts
- Transfers files from multiple hosts to a single target host, and stores the files on a local disk or locally attached storage device.
- Backs up data from remote hosts to a central host with locally-attached storage.
- Restores data from a central storage location to the remote hosts from which the data was originally retrieved.

Configuring Snap EDR for GuardianOS

To configure the SnapServer as a Management Console or an Agent, do the following:

1 Click the **Snap EDR** link in the Site Map (under **Extras**).

2 Select either the **Configure as the Management Console** or **Configure as the Agent** button.

Note If you are configuring the server as an Agent, you must provide the server name or IP Address of the Management Console.

3 Once the server is configured, a screen appears with the following options:

Option	Description
Click here to configure jobs	Opens the Management Console where jobs can be scheduled.
Stop Service	Stops all services.
Restart Service	Restarts all services. **Caution!** Use only if you have encountered a problem, and customer support advises you to restart the service. Any jobs currently running will stop and will not resume when you restart the service
Disable Service on System Boot	By default, when a user reboots the SnapServer, services automatically restart. Select **Disable Service on System Boot** if you do not want the Snap EDR service to start up automatically. **Note** When the disable service option is selected, the **Enable Service on System Boot** button appears.
Uninstall Service	Uninstalls all components of Snap EDR.

Scheduling Jobs in Snap EDR

To schedule jobs, click the **Snap EDR** link in the Site Map (under **Extras**).

For complete information on using Snap EDR, see the *Snap EDR Administrator's Guide*, available on the SnapServer website.

Off-the-Shelf Backup Solutions for the SnapServer

Note These backup packages do not support the backup of Windows ACLs or legacy POSIX ACLs. If you use one of these packages, Overland Storage strongly recommends you create a SnapServer disaster recovery image (see page 118) before you perform a backup.

In addition to the integrated backup solutions, GuardianOS supports a number of off-the-shelf backup packages that the user can install on the SnapServer, including:

- CA BrightStor ARCserver 11.5, 12.0
- EMC Legato NetWorker 7.3, 7.4
- Symantec Backup Exec 11d, 12, 12.5
- Symantec NetBackup 6.5

Note GuardianOS 5.0 and higher support the above versions of these backup solutions only.

Preparing to Install a Backup Solution

Before performing one of the backup solution installation procedures described here, make sure you have the following information and tools:

- **Backup and media server IP addresses —** Most backup agents need to know the IP addresses of the backup and media servers you plan to use with the SnapServer. Use the **Maintenance > Host File Editor** screen in the SnapServer's Administration Tool to supply a host-name-to-ip-address mapping that persists across system reboots.
- **SnapServer is seen by Backup software as a UNIX/Linux client —** When you configure a backup server to see the agent or client running on the SnapServer, assume the server is a UNIX or Linux client.
- **The agent/client files required by your backup software —** Typically, these files are either provided on your backup software's User CD or are available for download from the manufacturer's website. You will need to copy these files (usually delivered in a compressed format, e.g., as **.rpm*, **.tgz*, or **tar* files) to the SnapServer.
- **A secure shell (SSH) client —** To remotely install any backup solution on the SnapServer, you must have an SSH client installed on a remote workstation. The SnapServer SSH implementation requires SSH v2. If you do not already have an SSH client application installed, you can download one from the Internet.

  Note The commands you must enter via SSH to install your backup agent are case sensitive; pay careful attention to the capitalization of commands, and enter them exactly as shown.

- **Location of the SnapServer backup and restore path —** Backup servers often request the path for backup and restore operations on the SnapServer. When you configure a backup server to see the agent or client running on the SnapServer, use the following path:

  ```
  /shares/sharename
  ```

  where *sharename* is the name of the share to be backed up. If you have accepted the default SnapServer configuration, the correct path is as follows:

  ```
  /shares/SHARE1
  ```

- **Backup user account is configured to be exempt from password policies (if applicable) —** If the backup application uses a specific local Snap user account to perform backups, ensure that the user is exempt from password expiration policies, if enabled (see the Online Help for procedures to set password policy for local users).

Preinstallation Tasks

Perform the following tasks prior to installing any solution:

1. **Identify backup and media servers to the SnapServer.**

   In the Administration Tool, navigate to the **Maintenance > Host File Editor** screen and click **Add**. In the screen that opens, enter the IP address of the backup or media server; or enter one or both of the following as required by your backup software:

   - **Host name (long form)** Enter the fully qualified address for the backup server using the *myserver.mydomain.com* format.
   - **Host name (short form)** Enter an abbreviated address for the backup server using the *myserver* format.

   Click **OK**. The entry appears on the Host Editor screen. Repeat this procedure for each backup and media server you plan to use.

2. **Make sure SSH is Enabled on the SnapServer.**

   Navigate to the **Server > SSH** screen, make sure the **Enable SSH** box is checked, and then click **OK**. SSH is immediately available.

   Caution To maintain security, consider disabling SSH when not in use.

3. **On a client computer connected to the SnapServer, create a directory called *agent*.**

   You must create a directory to which you will copy the agent files. Create this directory on a client computer connected to the SnapServer. For purposes of illustration, the procedures described here assume that this directory is called *agent*.

4 **Copy the agent/backup files to the *agent* directory.**

Using a method appropriate to your environment, copy the agent/client files to the directory you just created for this purpose.

Installing the CA BrightStor ARCserve Agent

This section explains how to install the CA BrightStor ARCserve Agent versions 11.5 and 12.0.

Notes

- This procedure assumes that you are using the default SnapServer configuration; and you have created a directory called *agent* (to which to copy your agent/client files) on the default share (SHARE1), such that the path to the directory is */shares/SHARE1/agent*.
- Installing the BrightStor ARCserve backup agent on a SnapServer requires three agent (**.rpm*) files. These agent files are available from your BrightStor ARCserve CD, but some ARCserve CDs may not contain all the required files. To obtain the files you need, contact Computer Associates. If you have questions about the agent configuration, refer to your CA ARCserve documentation.

Prepare the SnapServer

1 Connect to the SnapServer via SSH.

Note SSH v2 is required. If you fail to connect to the server, ensure that your SSH client is configured to connect via SSH v2.

2 At the prompt, log in as admin, using the password you created for this account during the initial setup of the server.

3 You are placed into the CLI shell. However, a standard Linux shell must be used to install the agent. To launch a shell, type the following command and press Enter:

```
osshell
```

4 To change to superuser, enter the following command, and press Enter:

```
su -
```

5 At the prompt, enter the admin user password, and press Enter.

6 To change to the agent directory, type the following command and press Enter:

```
cd /shares/SHARE1/agent
```

7 To unpack the tar file to get the agent files, type the following command and press Enter:

```
tar -zxvf Linux.tar.Z
```

Note If you later delete the volume this directory is on, you will need to reinstall the agent.

8 Determine which volume has the most available space by looking at the `Avail` column in the volume usage table.

```
cd /hd
```

`ls` (lists all volumes)

`df -h` (shows volume usage)

9 Change directory to the volume with the most available space.

```
cd [volumename]
```

where ***[volumename]*** is the volume with the most available space

10 Create a directory `arcserve` on that volume.

11 Create the following symbolic links from the new directories in arcserve to the `/opt` directory:

```
ln -s /hd[volumename]/arcserve /opt/CA
```

Install CA ARCserve Agent

1 To install the agent files, enter the following command at the prompt, and press Enter:

```
rpm --nodeps -Uvh babagtux.rpm *lic*.rpm
```

2 Once the license is installed, run the Install script by entering the following command at the prompt and pressing Enter:

```
./install
```

Answer the prompts using the defaults.

Note You are installing the Linux Client Agent.

3 To change to the agent directory, enter the following command, and press Enter:

```
cd /opt/CA/BABuagent/
```

4 To run the setup program, enter the following command, and press Enter:

```
./uagentsetup
```

The BrightStorARCserve agent is now installed.

5 Enter the following command to run the script that will edit the agent.cfg file:

```
fix-arcserv
```

6 Close the SSH client and return to the Admnistration Tool. To start the newly installed backup agent, navigate to the **Maintenance > Shutdown/Restart** screen, and click **Restart**.

7 Delete the agent files you copied to the SnapServer because they are no longer needed.

8 To verify the success of the installation, use your backup management software to configure and run a test backup.

Uninstall CA ARCserve Agent

1 If you still have the tar or install directory that you copied to the SnapServer when you installed the ARCserve Agent, the uninstall script will be in that directory. If you do not have the directory or tar, copy the files again from the ARCserve CD or get them from Computer Associates.

2 Make sure you have the script `uninstall`. Type the following and follow the prompts:

```
./uninstall
```

Note Choose Option 1 to uninstall.

3 Uninstall the license `rpm` by typing the following:

```
rpm -e ca-lic
```

4 Verify that CA ARCserve Agent has been uninstalled by typing the following and verifying that you do not see the agents:

```
rpm -qa | grep BAB
```

Installing the Symantec Backup Exec RALUS Agent

To install the Backup Exec RALUS agent, do the following:

Prepare the SnapServer

1 Connect to the server over SSH.

Note SSH v2 is required. If you fail to connect to the server, ensure that your SSH client is configured to connect via SSH v2.

2 Log in as admin (using the password for the admin account).

3 You are placed into the CLI shell. However, a standard Linux shell must be used to install the agent. To launch a shell, type the following command and press Enter:

```
osshell
```

4 Change to root by entering the following command:

```
su -
```

Give the root password (same as admin password).

5 Select a volume on which to put a directory called *ralus*.

Note If you later delete the volume the *ralus* directory is on, you will need to reinstall the agent.

```
cd /hd
```

ls [lists all the volumes]

df -h [shows volume usage]

6 Determine which volume has the most available space by looking at the `Avail` column in the volume usage table. Change directory to the volume with the most available space.

```
cd [volumename]
```

where *[volumename]* is the name of the volume with the most available space.

7 Create a directory *ralus* on that volume:

```
mkdir ralus
```

8 In the *ralus* directory, create 3 directories called *VRTS*, *VRTSralus*, and *VRTSvxms*.

```
cd ralus
mkdir VRTS VRTSralus VRTSvxms
```

ls [to verify that the directories are there]

9 If CA Antivirus has been installed, you will have an */opt* directory. If it has not been installed, create an */opt* directory:

```
mkdir /opt
```

10 Create the following symbolic links from the new directories in *ralus* to the */opt* directory:

```
ln -s /hd/[volumename]/ralus/VRTS /opt
ln -s /hd/[volumename]/ralus/VRTSralus /opt
ln -s /hd/[volumename]/ralus/VRTSvxms /opt
```

where *[volumename]* is the name of the volume with the most available space.

11 Use the host file editor (**Maintenance > Host File Editor** screen) to add all the Backup Exec servers to **/etc/hosts** on the SnapServer, and verify that the agent server can ping the main Backup Exec server.

Note Do not edit the `/etc/hosts` file directly with a text editor.

Install Backup Exec RALUS Agent

1 From a network client, create a *ralusinstall* directory on SHARE1 of the SnapServer, then copy the RALUS agent tar file or contents of the RALUS agent CD to the directory.

2 If you copied the files from the CD, proceed to Step 3. If you downloaded the files from the Symantec website, in SSH, extract the files:

```
cd /shares/SHARE1/ralusinstall
tar -zxvf [filename].tar.gz
```

where *[filename]* is the name of the Backup Exec tar file.

3 Install the agent:

```
cd /shares/SHARE1/ralusinstall
```

(or other directory containing the CD contents)

```
./installralus
```

Follow the installation instructions, accepting the default options.

Note During the installation process, you may see an error message about the failure to add root to the *beoper* group. This error will be resolved in the following step.

4 Add the user *root* to the group *beoper* manually (or any other local Snap user you wish to use to perform backups):

```
cli group member add group-name=beoper user-name=root
```

Note If using a local Snap user account other than *root* or *admin*, and if password policies are enabled, configure the user to be exempt from password expiration. See "To Set Password Policy for Local Users" on page 68.

5 Start the Backup Exec RALUS agent by rebooting the SnapServer either through the Admin Tool (**Maintenance > Restart**), or by typing:

```
/etc/rc.d/init.d/VRTSralus.init start
```

6 Verify that using Backup Exec, you can create a job using the UNIX agent:

a Create a Guardian Root login account on the Backup Exec server.

b Connect as *root* (the password will be the same as the admin account password).

c Create a job and choose the Unix agent representing the SnapServer.

d Verify that you can connect to the agent, configure a job, and run the job.

Uninstall the Backup Exec RALUS AGENT

1 To uninstall the RALUS Agent, you will need the tar or install directory that you copied to the SnapServer when you installed the Agent (follow Steps 1 through 3 of Install Backup Exec RALUS Agent). Make sure you see the script `uninstallralus`

2 Type:

```
./uninstallralus
```

Follow the prompts.

3 Verify that the Symantec RALUS agent has been uninstalled by typing the following command:

```
rpm -qa | grep VRTS
```

Installing the Symantec NetBackup v6.5 Client

Note This procedure assumes that you are using the default SnapServer configuration; and you have created a directory called *agent* (to which to copy your agent/client files) on the default share (SHARE1), such that the path to the directory is */shares/SHARE1/agent*.

To install the Symantec NetBackup v6.5 Client, do the following:

Prepare the SnapServer

1 Connect to the server over SSH.

Note SSH v2 is required. If you fail to connect to the server, ensure that your SSH client is configured to connect via SSH v2.

2 Log in as admin (using the password for the admin account).

3 You are placed into the CLI shell. However, a standard Linux shell must be used to install the agent. To launch a shell, type the following command and press Enter:

```
osshell
```

4 Change to root by entering the following command:

```
su -
```

Give the root password (same as admin password).

5 Select a volume on which to put a directory called *openv*.

Note If you later delete the volume the *openv* directory is on, you will need to reinstall the agent.

`cd /hd`

`ls` [lists all the volumes]

`df -h` [shows volume usage]

6 Determine which volume has the most available space by looking at the `Avail` column in the volume usage table. Change directory to the volume with the most available space.

`cd [volumename]`

where *[volumename]* is the name of the volume with the most available space.

`ls` [lists what is on that volume]

7 Create a directory called *openv* on that volume:

```
mkdir openv
```

8 Create a "symbolic" link to the *openv* directory in the */usr/* directory:

```
ln -s hd/[volumename]/openv /usr/
```

where *[volumename]* is the name of the volume with the most available space.

9 Use the host file editor (**Maintenance > Host File Editor** screen) to add the NetBackup servers to **`/etc/hosts`** on the SnapServer. Verify that you can ping the NetBackup server.

Install NetBackup v6.5 Client

1 Using a network client, copy the directory called `NBClients` from the Client CD to a directory on a share (e.g., SHARE1 or Agent) on the SnapServer.

2 In SSH, install the files:

```
cd /shares/SHARE1/NBClients/catalog/anb
./client.inst
```

Follow the instructions, choosing RedHat Linux (choose 2.6 kernel version, if available) as the type.

3 Once the NetBackup Client is installed, reboot the server using the Administration Tool (**Maintenance > Restart**) to start the client service.

4 Verify that you can configure the UNIX client:

a Create a policy and add the SnapServer as a client.

b Look at the client list to verify that the SnapServer client is listed.

Uninstall the NetBackup v6.5 Client

1 Log in to the client system as the root user.

2 Navigate to the volume where you installed the NetBackup directory.

```
cd /hd/vol_mnt[X]/
rm -rf /usr/openv/
rmdir openv/
```

3 Remove the NetBackup entries in the client's `/etc/services` file.

Locate the lines, marked by the following strings and delete them:

```
# NetBackup services#.....# End NetBackup services #
```

4 Remove the NetBackup services by deleting the files for `bpcd`, `vnetd`, `vopied`, and `bpjava-msvc` in the `/etc/xinetd.d/` directory.

```
rm -rf /etc/xinetd.d/bpcd
rm -rf /etc/xinetd.d/vnetd
rm -rf /etc/xinetd.d/vopied
rm -rf /etc/xinetd.d/bpjava-msc
```

5 Restart the SnapServer services by either rebooting or typing:

```
/etc/rc.d/init.d/xinetd reload
```

Installing the EMC Legato NetWorker Client

Note This procedure assumes that you are using the default SnapServer configuration; and you have created a directory called *agent* (to which to copy your agent/client files) on the default share (SHARE1), such that the path to the directory is /*shares/SHARE1/agent*.

This section describes how to install the EMC Legato NetWorker UNIX/Linux client, as well as special procedures EMC Legato NetWorker users must follow in order to perform backup and restore operations on the SnapServer.

Prepare the SnapServer

1 Connect to the server over SSH.

Note SSH v2 is required. If you fail to connect to the server, ensure that your SSH client is configured to connect via SSH v2.

2 Log in as admin (using the password for the admin account).

3 You are placed into the CLI shell. However, a standard Linux shell must be used to install the agent. To launch a shell, type the following command and press Enter:

```
osshell
```

4 Change to root by entering the following command:

```
su -
```

Give the root password (same as admin password).

5. Select a volume on which to put a directory called *networker*.

   Note If you later delete the volume the *networker* directory is on, you will need to reinstall the agent.

   ```
   cd /hd
   ```

   `ls` [lists all the volumes]

   `df -h` [shows volume usage]

6. Determine which volume has the most available space by looking at the `Avail` column in the volume usage table. Change directory to the volume with the most available space.

   ```
   cd [volumename]
   ```

   where *[volumename]* is the name of the volume with the most available space.

7. Create a directory *networker* on that volume:

   ```
   mkdir networker
   ```

8. In the *networker* directory, create the following directories called *opt*, *usr*, and *opt/usr*.

   ```
   cd networker
   mkdir opt usr opt/usr
   ```

   `ls` [to verify that the directories are there]

9. If CA Antivirus has been installed, you will have an */opt* directory. If it has not been installed, create an */opt* directory:

   ```
   mkdir /opt
   ```

10. Create links from the *networker* working volume to the root filesystem:

    ```
    ln -s /hd/vol_mnt[X]/networker/nsr/
    ln -s /hd/vol_mnt[X]/networker/opt/nsr /opt/
    ln -s /hd/vol_mnt[X]/networker/usr /usr/
    ```

    where *vol_mnt[X]* is the NetWorker installation target volume.

11. Modify the SnapServer environment by editing */etc/profile* as follows:

    ```
    cp /etc/profile /etc/profile.nwbk
    echo PATH=$PATH:/hd/vol_mnt[X]/networker/usr/bin:/hd/vol_mnt{X]/
    networker/usr/sbin:/hd/vol_mnt[X]/networker/usr/lib >> /etc/
    profile
    ```

    where *vol_mnt[X]* is the NetWorker installation target volume.

    Note Be sure to enter '`>>`' in the command rather than '`>`' or you will overwrite the file rather than append to the */etc/profile* script. If you need to redo Step 11, copy the backup to the original using the command **`cp /etc/profile.nwbk /etc/profile`** and then edit the file again.

12 To implement the changes, enter the following command:

```
source /etc/profile
```

Install the EMC Legato Networker Client

1 Connect to the SnapServer via SSH, and log in as admin, using your admin user password.

Note SSH v2 is required. If you fail to connect to the server, ensure that your SSH client is configured to connect via SSH v2.

2 You are placed into the CLI shell. However, a standard Linux shell must be used to install the agent. To launch a shell, type the following command and press Enter:

```
osshell
```

3 To change to superuser, enter the following command, and press Enter:

```
su -
```

4 At the prompt, enter the admin user password, and press Enter.

5 Use the **`cd`** command to change to the directory in the share, for example:

```
cd /shares/SHARE1/agent
```

6 To unpackage the client files, enter the following commands:

```
tar xvfz nw_linux86.tar.gz
```

7 To install the NetWorker Agent rpm, enter the following command:

```
rpm -Uvh --nodeps --relocate=/usr/=/hd/vol_mnt[X]/NetWorker/usr/
lgtoclnt-X.X-X.i686.rpm
```

where *vol_mnt[X]* is the NetWorker installation target volume and *x.x-x* is the version number.

8 To start the EMC Legato NetWorker daemon, enter the following command at the console:

```
/etc/rc.d/init.d/networker start
```

The NetWorker client is now installed.

9 Close the SSH client, return to the Administration Tool. To start the newly installed backup agent, navigate to the **Maintenance > Shutdown/Restart** screen, and click **Restart**.

10 Delete the client files you copied to the SnapServer because they are no longer needed.

11 To verify the success of the installation, use your backup management software to configure and run a test backup.

Backup and Restore Operations with the EMC Legato NetWorker Client

This section describes special procedures EMC Legato NetWorker users must use in order to perform backup and restore operations on the SnapServer.

Add the SnapServer as a Root User

For backup operations, NetWorker requires that the SnapServer be configured as a root user. To add the SnapServer root user as one of the administrators, use the following procedure:

1. Open the NetWorker Administrator application.
2. Click the **Configuration** tab.
3. Click the **User Groups** menu item.
4. Click on the **Administrators** group.
5. In the Configuration box, add one of the following:

   `user=root@`*`hostname`*

   where *hostname* is the host name of the SnapServer for each SnapServer.

   Or, enter:

   `user=root`

   to add root for all SnapServers.
6. Click **OK**.

Recover and Retrieve Operations

The EMC Legato NetWorker administrative interface does not support data recovery operations from a remote client for a Linux-based operating system such as the GuardianOS. To recover data, you must execute one of the following CLI commands from a SSH client.

- **Recover —** The **`recover`** command restores data from a normal backup job.
- **Nsrretrieve —** The **`retrieve`** command restores data from an archive.

Use either the **recover** or the **retrieve** command exactly as described below. For more details on these commands, see the *EMC Legato Networker Command Reference*.

1 Connect to the SnapServer via SSH, and log in using the admin user name and password.

  Note SSH v2 is required. If you fail to connect to the server, ensure that your SSH client is configured to connect via SSH v2.

2 You are placed into the CLI shell. However, a standard Linux shell must be used to install the agent. To launch a shell, type the following command and press Enter:

  ```
  osshell
  ```

3 To change to superuser, enter the following command, and press Enter:

  ```
  su -
  ```

4 At the prompt, enter the admin user password, and press Enter.

5 **To recover data from a normal backup operation**, enter one of the following commands, and press Enter:

  - To recover data to its original location:
    recover -s *backupservername* **-c** *snapservername* **-f -i "/shares/** *SHARE1/data/***" -a**
    where **/shares/***SHARE1/data* is the path of the data you are restoring.

  - To recover data to a different location:
    recover -s *backupservername* **-c** *snapservername* **-f -i -a R -d "/shares/***SHARE1/relocated_data/***" "/shares/***SHARE1/Data/***"**
    where **/shares/***SHARE1/relocated_data/* is the path to the new target location for the restore operation; and where **/shares/***SHARE1/Data/* is the path of the data you are restoring.

6 **To retrieve data from an archival backup operation**, enter one of the following commands, and press Enter:

  - To retrieve data to its original location:
    nsrretrieve -f -i -s *backupservername* **-A** *annotation* **"/shares/** *SHARE1/data/"*
    where **/shares/***SHARE1/data/* is the path of the data you are restoring.

  - To retrieve data to different location:
    nsrretrieve -f -iR -d "/shares/*SHARE1/new_dir"* **-s** *backupservername* **-A** *"annotation"* *"***/shares/***SHARE1/Data/***"**
    where **/shares/***SHARE1/new_dir"* is the path to the new target location for the restore operation; where *annotation* is the name of the EMC Legato backup; and**/shares/***SHARE1/Data/"* is the path of the data you are restoring.

Backup of iSCSI Disks

iSCSI disks can be backed up from iSCSI clients using any standard backup application on the client operating system. These backups run independently of the SnapServer since the client backs up the contents of the iSCSI disk as if the iSCSI disk were a local hard disk.

Windows clients can make backups of VSS-based snapshots of iSCSI disks using VSS-compatible backup applications. See “Backing up an iSCSI Disk using VSS Snapshots” on page 141 for instructions.

Using Backup Exec to Take VSS-based Snapshots of SnapServer iSCSI Disks

To configure Backup Exec to take native VSS snapshots of SnapServer iSCSI disks using Backup Exec’s *Advanced Open File* or *Advanced Disk-Based Backup* feature, you must first add a Windows registry entry to the systems running the Backup Exec Server and all of the Backup Exec agents backing up iSCSI disks.

After the Backup Exec Server or agent has been installed, modify the registry to add the SnapServer as a Backup Exec VSS provider:

1 Run the following command:

```
regedit
```

2 Navigate to the following key:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Backup Exec For
Windows\Backup Exec\Engine\Misc\VSSProviders]
```

3 Underneath VSSProviders are other keys numbered sequentially from 0 to some number. Create a new key in VSSProviders named after the highest key value plus 1 (i.e., if the highest key value is *9*, create a new key value *10*). For example:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Backup Exec For
Windows\Backup Exec\Engine\Misc\VSSProviders]\10
```

4 Inside the new key, create three string values:

VALUE NAME	**VALUE DATA**
Id	**{759c7754-6994-46c9-9cf9-c34ac63a0689}**
Name	**SnapServer VSS Hardware Provider**
Version	**5.2**

5) Close `regedit`.

The Snap VSS Provider should now be available to Backup Exec to use for VSS-based backups.

Command Line Interface

GuardianOS includes a command line interface (SnapCLI) accessible through SSH. Using the CLI, users can access information about most of the SnapServer configuration parameters and perform configuration and maintenance functions without using the GuardianOS web interface or SSM.

Note Some administrative tasks must still be performed using the Administration Tool. The CLI is intended as a convenient way to perform some functions; it is not intended as an alternative to using the GUI.

Topics in Command Line Interface

- SnapCLI Syntax
- SnapCLI Commands
- Scripts in SnapCLI

SnapCLI Syntax

SnapCLI command syntax uses three parameters: COMMANDS, ARGUMENTS, and OPTIONS. To generate commands in SnapCLI, use the following syntax:

```
COMMAND [ARGUMENT] [OPTIONS]
```

where `COMMAND` is the name of one of the SnapCLI commands, `ARGUMENT` is an action available for that command, and `OPTIONS` are additional parameters for the command.

Once logged into the CLI, there are several ways of displaying information about available parameters.

Type	To...
?	see an overview of the CLI, with a list of available commands and a description of command syntax.
***{command}* help**	see a description of that particular command's function and a list of options available for the command.
tab	finish the command you have started to type (i.e., tab-complete).
***{command}* tab**	list any arguments and/or options available for that command.

For example, to see a list of available commands once you have logged into SnapCLI, type **?** at the prompt.

To see a description of a specific command, type the command name (e.g., date) + help or ?:

```
date help
```

Command	Arguments and Options	Descriptions
date	**timezones**	- list available time zones
	get	- get server date/time
	set [OPTIONS} - [day=1-31] - [month=1-12] - [year=1900-...] - [hour=0-23] - [minute=0-59] - [second=0-59] - [timezone=1-...]	- set server date/time - day of month - month of year - year - hour - minutes - seconds - timezone (use the command **date timezones** to get a list of timezones)

In this instance, to set the date to February 27, 2007, enter:

```
date set day=27 month=2 year=2007
```

Note If, instead of typing the word `date`, you had typed **d + [tab]**, the word would have been completed for you. If you entered **d + [tab] + [tab]**, the word would have been completed and the available options displayed.

Suppose, instead of `date`, you entered the command `web`. Two arguments would be available, one with options:

Command	Arguments and Options	Descriptions
web	**get**	- get WEB properties
	set [OPTIONS]	- set WEB properties
	- require-webview-auth=(yes|no)	- require HTTP/HTTPS clients to authenticate in order to accesss the server
	- non-secure-http=(yes|no)	-enable/disable non-secure HTTP access

Thus, the following command string:

```
web set require-webview-auth=yes non-secure-http=no
```

sets HTTP/HTTPs properties on the SnapServer to require clients to authenticate in order to access the server and to disable non-secure HTTP access.

Procedures

Logging into SnapCLI

1 Make sure your client has an SSH v2 client application installed.

Note Free or low-cost SSH applications are available over the Internet.

2 Connect to the server using its name or IP address, and log in as *admin* (or any other member of *admingp*).

You will automatically be placed in the CLI shell.

Note SSH v2 is required. If you fail to connect to the server, ensure that your SSH client is configured to connect via SSH v2.

Exiting SnapCLI

To exit SnapCLI, type `exit`. The SSH session will close.

SnapCLI Commands

The following table presents a list of the available SnapCLI commands and a brief description of the function of each.

Command	Description
activeusers	Display active users
apple get	Display apple network settings
apple set	Update apple network settings
date get	Get the current date/timezone information
date set	Set the current date/timezone information
date timezones	List the available timezones (used in conjunction with the date set command)
dhcp get	Display DHCP server settings
dhcp set	Update DHCP server settings
diskunits	Get status information of all the disk units on the server
domain get	Get the domains known to the SnapServer and their properties
domain list	List the domains known to the SnapServer
dri create	Create a Disaster Recovery Image (dri)
dri recover system	Restore a Disaster Recovery Image (dri)
dri recover volume	Restore a Disaster Recovery Volume Image (dri)
email get	Get email notification settings
email set	Set email notification settings
event clear	Clear all events in the System Event Log
event get	Display the System Event Log
factorydefaults	Reset the SnapServer's settings back to the factory defaults, will reboot
ftp get	Get the current ftp settings, including anonymous user access
ftp set	Set the current ftp settings, including anonymous user access
globalspares list	List global hot spares
globalspares remove	Remove a disk from the global spares list
globalspares add	Add a disk to the global spares list

Command	Description
group create	Create a local group
group delete	Delete a local group
group get	Get available groups with their associated information
group list	List available groups
group set	Change the properties of a local group
group member add	Add a group member to a local group
group member delete	Delete a group member from a local group
group members get	Get a list of the members of a local group
group members list	List the members of a local group
homedirs get	Get Home Directory configuration information
homedirs set	Set Home Directory configuration information
hostfile add	Add a host file entry
hostfile delete	Delete a host file entry
hostfile get	Get information for a specific host file entry
hostfile set	Set information for a specific host file entry
hostfile list	List all host file entries
idmap auto map	View/Save auto-generated ID mappings
idmap count	Count number of ID mappings
idmap group get	Get ID mapping for a (windows domain) group
idmap group remove	Remove ID mapping for a (windows domain) group
idmap group set	Set ID mapping for a (windows domain) group to a local or NIS group
idmap list	List all ID mappings
idmap remove all	Remove all ID mappings
idmap update files	Update filesystem for ID mapping changes
idmap update status	View status of ID mapping update filesystem operation
idmap user get	Get ID mapping for a (windows domain) user
idmap user remove	Remove ID mapping for a (windows domain) user
idmap user set	Set ID mapping for a (windows domain) user to a local or NIS user
iscsi create	Create an iscsi disk

Command	Description
iscsi delete	Delete an iscsi disk
iscsi get	Get iscsi disk properties
iscsi set	Set iscsi disk properties
isns get	Get configuration settings for iSNS server
isns set	Set configuration settings for iSNS server
jumboframe get	Get jumbo frame settings for all interfaces
jumboframe list	List jumbo frame settings for all interfaces
jumboframe set	Set jumbo frame settings for all interfaces
name get	Get the name of the SnapServer
name set	Set the name of the SnapServer
netinfo	Get information about the Ethernet interface
nfs get	Get SnapServer NFS Properties
nfs set	Set SnapServer NFS Properties
nis get	Get current NIS settings
nis set	Set current NIS settings
ntp get	Get NTP client settings
ntp set	Set NTP client settings
ntp_server get	Get NTP Server settings
ntp_server set	Set NTP Server settings
openfiles	List the Open Files
osupdate get	Display status of last OS update
osupdate load	Perform an OS update
passwordpolicy get	Display Password Policy settings and status
passwordpolicy set	Update Password Policy settings
phonehome	Send configuration details to SnapServer Technical Support
proxy get	Display the HTTP proxy properties
proxy set	Set the HTTP proxy properties
quota list	List user or group quotas for a volume
quota get	Get quota settings for a volume
quota set	Set quota settings for a volume
quota group get	Get volume quota limit & usage for a specific group

Command	Description
quota group set	Set volume quota limit & usage for a specific group
quota user get	Get volume quota limit & usage for a specific user
quota user set	Set volume quota limit & usage for a specific user
raid list	List available raids
raid create	Create a raid set
raid delete	Delete a raid set
raid get	Get raid set properties
raid add disk	Add a disk to a raid set
raid remove disk	Remove a disk from a raid set
raid repair	Repair a degraded raid set
raidsettings get	Get auto-incorporation and back-round disk settings
raidsettings set	Set the auto-incorporation and background disk properties
reboot	Reboot the SnapServer
registration get	Get registration status
registration set	Set registration key
securitymodel get	Get the security model on a SnapServer Volume
securitymodel set	Set the security model on a SnapServer Volume
share create	Create a share
share delete	Delete a share
share get	View a share
share rename	Rename a share
share set	Modify a share
share list	List available shares
share access get	Get access list for the share
share access set	Set access list for the share
share access delete	Delete access permission of the specified user/group for the share
share nfsaccess get	Get NFS access permission of the host for the specified share
share nfsaccess set	Set NFS access permission of the host for the specified share

Command	Description
share nfsaccess delete	Delete NFS access permission of the host for the specified share
shutdown	Shutdown the SnapServer
slidingwindow get	Get sliding window settings for a specific interface
slidingwindow set	Set sliding window settings for a specific interface
slidingwindow list	List sliding window settings for all interfaces
snapex	Perform a control operation on the snap extension
snapshot create later	Create a new snapshot schedule
snapshot get	Get snapshot properties
snapshot set	Set properties for the specified snapshot
snapshot list	Get list of snapshots
snapshot create now	Create a new one time snapshot to be run immediately
snapshot delete	Delete specified snapshot
snapshot sched delete	Delete specified snapshot schedule
snapshot sched get	Get specified snapshot schedule
snapshot sched set	Set specified snapshot schedule
snapshot sched list	List current snapshot schedules
snapshot pool get	Get snapshot pool properties
snapshot pool set	Set snapshot pool properties
snapshot pool list	List current snapshot pools
snapshot rollback	Start a rollback for the specified snapshot
snmp get	Get SNMP parameters
snmp set	Set SNMP parameters
ssh get	Get current SSH settings
ssh set	Enable and Disable SSH. **Caution** Turning off SSH while running the command line will 'kick' the user off the system and they won't be able to log back into the command line until SSH is re-enabled via the SnapServer Web Administration
syslog all	Create a tar file of syswrapper and all third party logs
syslog edr	Create a tar file of Snap EDR logs
syslog netvault	Create a tar file of NetVault logs

Command	Description
syslog s2s	Create a tar file of S2Sv2 logs
syslog syswrapper	Create a tar file of syswrapper only
systemstatus	Get system status information for the server
tape list	List the SCSI tape devices
tape settings get	Display current SCSI tape device settings
tape settings set	Update SCSI tape device settings
tcpip get	Get TCP/IP parameters
tcpip set	Set TCP/IP parameters. **Caution** Changing the parameters of the ethernet interface over which the user is currently running the SSH/command line session may result in the user being disconnected.
tcpip create bond	Create a bond and set TCP/IP properties.
tcpip delete bond	Remove a TCP/IP bond.
unicode get	Get current Unicode settings
unicode set	Enable Unicode on the system
updatenotification get	Get update notification properties
updatenotification set	Set update notification properties
updatenotification check	Check to see if updates are available
ups get	Get UPS settings and status
ups set	Set UPS settings
user create	Create a local user
user delete	Delete a local user
user get	Get available users with their associated information
user list	List available users
user set	Change the properties of a local user
user lock	Lock the specified user.
user unlock	Unlock the specified user.
version	Display current version information, including the Server Number. **Note** This is the same information displayed in the Web Administration "About" box
volume list	List of the the volumes defined on the SnapServer

Command	Description
volume get	Get a specific volume’s properties
volume create	Create a new logical volume
volume edit	Edit an existing logical volume
volume delete	Delete a logical volume
volume fscheck	Check or repair filesystem
volume fscheck-root	Repair root filesystem (requires reboot)
volume write-cache	Enable or disable write cache on a volume.
vxxaccess list	List hostnames with VSS/VDS access
vxxaccess add	Add hostname of VSS/VDS client requiring access to this server
vxxaccess delete	Delete access for a VSS/VDS client hostname
web get	Get current HTTP Web access settings
web set	Enable or Disable HTTP access to Web Administration interface
windows get	Get windows network settings
windows set	Set windows network settings
clear	Clear the screen
exit	Quit the command line, log off, and exit ssh/bash session. **Note** If user has started another shell, the command 'exit' will return them to the SnapServer command line shell.
history	Print the history of commands typed into the SnapServer command line
less	With a file name, this command allows the user to view any file on the system. It should only be used for 'text' files.
Quit	Quit the command line, log off, and exit the ssh/bash session

Scripts in SnapCLI

Administrative tasks can be automated with shell scripts that call SnapCLI commands.

Running a SnapCLI Script

1 Create the script and put it in a share on the local server.

   Notes

   - Be sure to use an application that is compatible with the standard UNIX text file format (e.g., *vi*). Avoid using Windows clients to create or edit scripts.
   - Place the script in a share that will never be part of a delete script.

2 Log in to the SnapCLI (see Logging into SnapCLI for instructions).

3 Type `osshell` to get a bash prompt.

4 At the prompt, make sure the script is executable by typing the following and pressing Enter:

```
chmod +x/shares/[sharename]/[scriptname]
```

   where *sharename* is the name of the share where you put the script and *scriptname* is the name of the script.

5 To run the script, type the path again, and press Enter:

```
/shares/[sharename]/[scriptname]
```

Sample Script

Following is an example script that can be used to create and remove users, groups, and shares:

```
#!/bin/sh
##########################################################
# Copyright 2003-2007 Overland Storage, Inc. All rights reserved. #
# Permision is granted to use this code provided that it #
# retains the above copyright notice.                    ##
##########################################################
CLI=/bin/cli
USER=myuser
PASSWORD=myuserpass
GROUP=mygroup
SHARE=myshare
VOLUME=VOL0

# usage: 'mkuser <user_name> <password>'
mkuser()
{
```

Create a user

```
# if the user does not exist then create it
if ! $CLI user get user-name="$1" > /dev/null 2>&1; then
echo "Creating user '$1' ..."
$CLI user create user-name="$1" password="$2" > /dev/null 2>&1
if [ $? -ne 0 ]; then
echo "Creation of user '$1' failed."
return 1
fi
else
echo "User '$1' already exists."
fi

return 0
}


# usage: 'mgroup <group_name>'
mkgroup()
{
```

Create a group

```
# if the group does not exist then create it
if ! $CLI group get group-name="$1" > /dev/null 2>&1; then
                echo "Creating group '$1' ..."
        $CLI group create group-name="$1" > /dev/null 2>&1
        if [ $? -ne 0 ]; then
                echo "Creation of group '$1' failed."
return 1
        fi
else
echo "Group '$1' already exists."
fi

return 0
}


# usage: 'adduser2group <user_name> <group_name>'
adduser2group()
{
```

Add the user to the group

```
# if both the user and the group exist add the user as a member of this group
if $CLI user get user-name="$1" > /dev/null 2>&1; then
if $CLI group get group-name="$2" > /dev/null 2>&1; then
echo "Adding user '$1' to group '$2' ..."
$CLI group member add user-name="$1" group-name="$2" > /dev/null 2>&1
        if [ $? -ne 0 ]; then
                echo "Adding user '$1' to group '$2' failed."
return 1
        fi
fi
fi

return 0
}


# usage: 'mkshare <share_name> <share_volume>'
mkshare()
{
```

Create a share

```
# if the share does not exist create it
if ! $CLI share get share-name="$1" > /dev/null 2>&1; then
echo "Creating share '$1' ..."
$CLI share create share-name="$1" share-volume="$2" > /dev/null 2>&1
       if [ $? -ne 0 ]; then
                echo "Creating share '$1' failed."
return 1
        fi
else
echo "Share '$1' already exists."
fi

return 0
}


# usage: 'rmuser <user_name>'
rmuser()
{
```

Delete the user

```
# if the user exists then delete it
if $CLI user get user-name="$1" > /dev/null 2>&1; then
echo "Deleting user '$1' ..."
        $CLI user delete user-name="$1" > /dev/null 2>&1
        if [ $? -ne 0 ]; then
                echo "Deletion of user '$1' failed."
return 1
        fi
else
        echo "User '$1' does not exist."
fi

return 0
}


# usage: 'rmgroup <group_name>'
rmgroup()
{
```

Delete the group

```
# if the group exists then delete it
if $CLI group get group-name="$1" > /dev/null 2>&1; then
echo "Deleting group '$1' ..."
```

```
        $CLI group delete group-name="$1" > /dev/null 2>&1
        if [ $? -ne 0 ]; then
                echo "Deletion of group '$1' failed."
return 1
        fi
else
        echo "Group '$1P' does not exist."
fi

return 0
}


# usage: 'rmshare <share_name>'
rmshare()
{
```

Delete the share

```
# if the share exists delete it
if $CLI share get share-name="$1" > /dev/null 2>&1; then
echo "Deleting share '$1' ..."
        $CLI share delete share-name="$1" > /dev/null 2>&1
        if [ $? -ne 0 ]; then
                echo "Deletion of share '$1' failed."
return 1
       fi
else
        echo "Share '$1' does not exist."
fi

return 0
}
```

Create a user, group, and share; then add the user to the group

```
##############
#    Main    #
##############

# create a user, a group and a share and add the user to the group
mkuser "$USER" "$PASSWORD"
mkgroup "$GROUP"
adduser2group "$USER" "$GROUP"
mkshare "$SHARE" "$VOLUME"

#remove the group, the user and the share
rmgroup "$GROUP"
rmuser "$USER"
rmshare "$SHARE"
```

Troubleshooting SnapServers

Basic techniques for identifying and resolving common hardware and networking issues are described here.

Topics in Troubleshooting SnapServers

- The Meaning of LED Indicators
- System Reset Options
- Networking Issues
- Miscellaneous Issues
- Phone Home Support

Additional Resources

Resource	Description
Knowledge Base	Search for solutions to specific issues by clicking the **Knowledge Base** link on the SnapServer support page: http://www.snapserver.com/kb
Hardware Components	Purchase additional hardware components from authorized SnapServer resellers.To locate a reseller in your area, select the **How to Buy** tab on the SnapServer home page: http://www.snapserver.com
Field Service Documents	Find a list of the hardware components available for your SnapServer or expansion array by navigating to the server or expansion array model: http://www.snapserver.com Procedures to install or replace components are available from the SnapServer support page: http://www.overlandstorage.com/support/crscd

The Meaning of LED Indicators

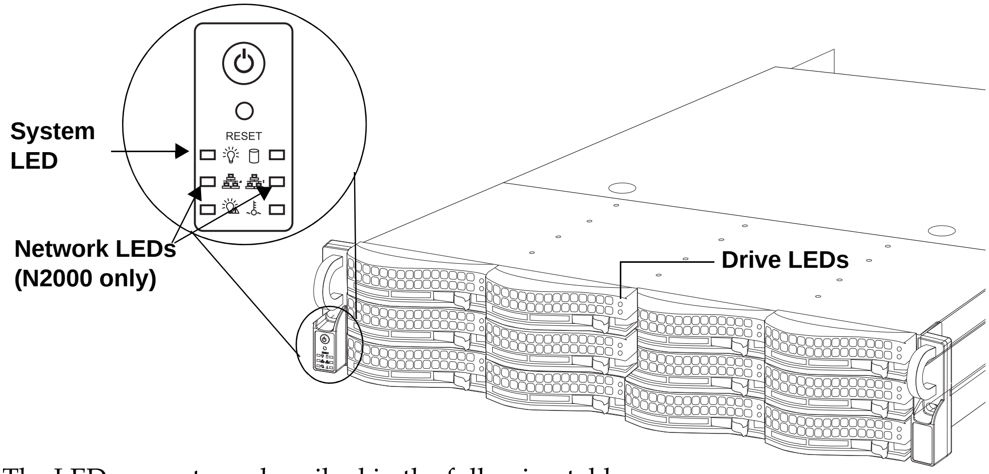
LED indicators provide information on the status of basic connectivity, disk drives, fan modules, and power supply modules.

- SnapServer NAS N2000 and EXP E2000 Status and Drive Light Behavior
- SnapServer 110/210 Status and Drive Light Behavior
- SnapServer 410 Status and Drive Light Behavior
- SnapServer 500/600 Series Status and Drive Light Behavior
- SnapServer 4200/4500 Status and Drive Light Behavior
- SnapServer 18000 Status and Drive Light Behavior
- Snap Expansion S50 Enclosure, Disk Drive, APC Module, and Controller Behavior
- Snap Disk 10 Disk Drive and Power Supply Module LEDs
- Snap Disk 30SA Disk Drive and Power/Fan Module Behavior

SnapServer NAS N2000 and EXP E2000 Status and Drive Light Behavior

The SnapServer NAS N2000 has one System light, two Network lights (Ethernet1, left; Ethernet2, right), and two disk lights per disk drive, as shown in the following illustration.

The SnapServer EXP E2000 has one System light and two Drive lights per drive.



The LEDs operate as described in the following tables:

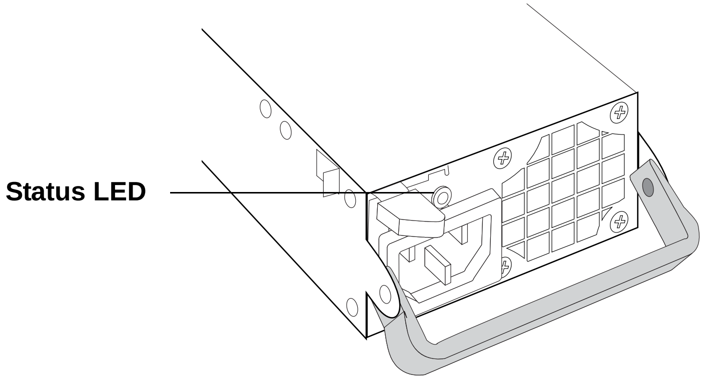
System LED	
Solid green	The unit is powered on but GuardianOS is not running.
Blinking green (N2000 only)	GuardianOS is booted and operating normally.

Network LEDs (N2000 only)	
Solid green	The server is active and connected to the network.
Off	The port is disconnected or the Ethernet cable is not connected or linked to an active switch.

Disk LEDs		
Top LED	Off (SATA drive) Solid Blue (SAS drive)	Disk drive installed properly but is not active
	Blinking Blue	Disk drive installed properly and is active
Bottom LED	Solid Red	Disk drive error
All Drive LEDs (E2000 only)	Blinking simultaneously	UID identification from Disks/Units page of Admin Tool.

Power Supply Module Indicator Lights

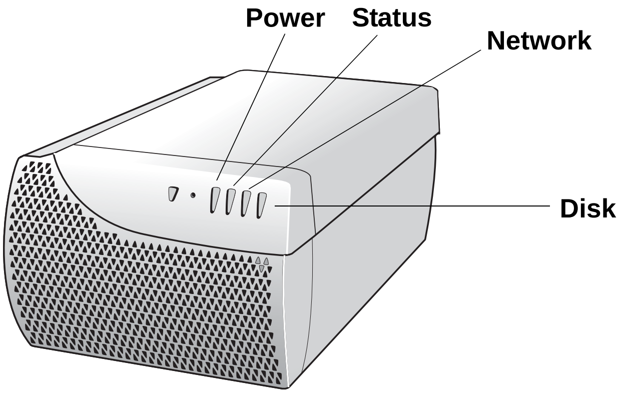
The LED on a SnapServer N2000 and E2000 power module is identified in the following illustration.



Power	Description
Solid green	The module is operating properly.
Solid amber **Off**	The module has failed, is not connected, or the server has been turned off.

SnapServer 110/210 Status and Drive Light Behavior

The server has two status lights, one network light, and one disk light, as shown in the following illustration:



Power and System LEDs

These status lights are located to the right of the power button. Looking at the server from the front, the lights appear in the following order, from left to right: Power LED, Status LED, Network LED, and Disk LED.

The LEDs operate as described in the following tables:

Power LED	
Solid green	The server is powered on.
Off	The server is powered off.

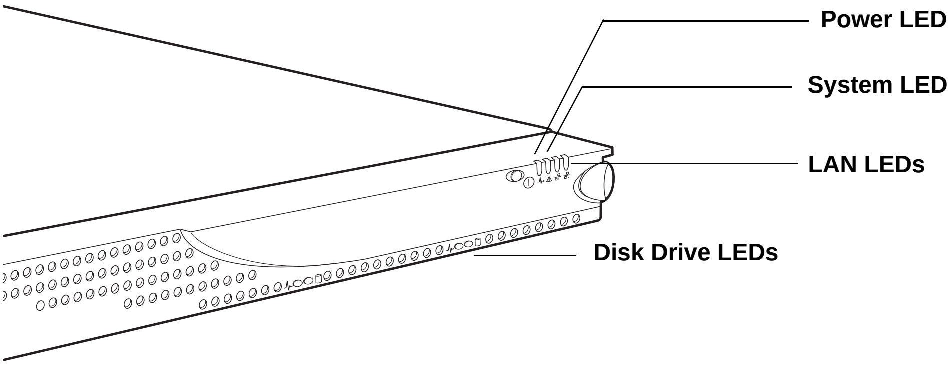
Status LED	
Blinking green	The server is operating normally.
Blinking amber	A thermal or other system problem was detected.
Blinking amber and green	The server is in Maintenance Mode.

Network LED	
Solid green	The server is active and connected to the network.
Off	The port is disconnected or the Ethernet cable is not connected or linked to an active switch.

Disk LED	
Blinking green	Disk drive is active.
Solid amber	Disk drive error.
Off	No disk drive activity.

SnapServer 410 Status and Drive Light Behavior

The server has two status lights, two network lights, and two lights for each of the four disk drives, as shown in the following illustration:



Overland Storage recommends that you become familiar with the operation of these lights.

Power, System, and LAN LEDs

These status lights are located to the right of the power button. Looking at the server from the front, the lights appear in the following order, from left to right: power LED, system LED, LAN 1 (Ethernet1) LED, and LAN 2 (Ethernet2) LED. The Disk Drive LEDs run along the bottom of the bezel, two LEDs for each disk drive.

The LEDs operate as described in the following tables:

Power LED	
Solid green	The server is powered on.
Off	The server is powered off.

System LED	
Blinking green	The server is operating normally.
Blinking amber	A thermal or other system problem was detected.
Blinking amber and green	The server is in Maintenance Mode.

LAN 1 and LAN 2 LEDs	
Solid green	The server is active and connected to the network.
Off	The port is disconnected or the Ethernet cable is not connected or linked to an active switch.

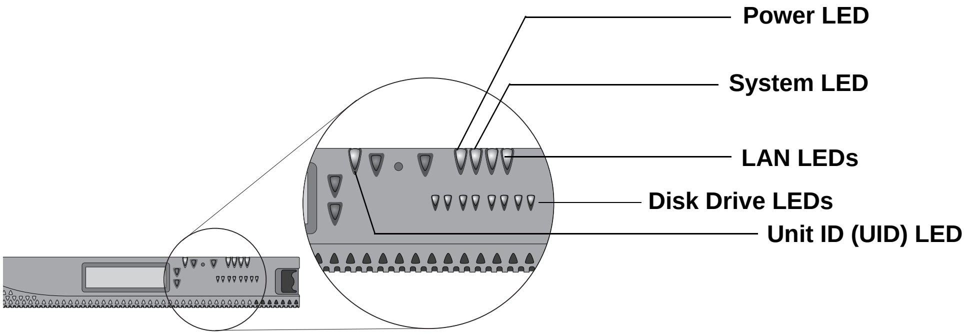
Disk Drive LEDs

Disk drive LEDs are located along the bottom of the bezel, two LEDs for each drive. For all disk drive LEDs, the left light indicates drive status; the right light indicates drive activity. They operate as follows:

Status LED (left)	**Activity LED (right)**	
Off	Off	Drive is not present.
Solid green	Blinking green	Disk drive installed properly and is active
Solid amber	Off	Disk drive installed, but not working correctly

SnapServer 500/600 Series Status and Drive Light Behavior

The server has two status lights, two network lights, two lights for each of the four disk drives, and an identification light, as shown in the following illustration:



Overland Storage recommends that you become familiar with the operation of these lights.

Power, System, and LAN LEDs

These status lights are located to the right of the power button. Looking at the server from the front, the lights appear in the following order, from left to right: power LED, system LED, LAN 1 (Ethernet1) LED, and LAN 2 (Ethernet2) LED. The Disk Drive LEDs are below the status lights, and the indentification (Unit ID) LED is to the right of the LCD display.

The LEDs operate as described in the following tables:

Power LED	
Solid green	The server is powered on.
Off	The server is powered off.

System LED	
Double-blink green	The server is booting up.
Triple-blink green	The server is shutting down.
Solid or blinking amber at boot time	A problem was detected. The server will not boot.
Blinking amber during normal operation	A thermal or other system problem was detected.
Blinking amber and green	The server is in Maintenance Mode.

LAN 1 and LAN 2 LEDs	
Solid green	The server is active and connected to the network.
Off	The port is disconnected or the Ethernet cable is not connected or linked to an active switch.

Unit ID (UID) Front and Back LEDs	
Blue	Unit ID is on and identifies the unit (front and back).
Off	Unit ID has not been turned on.

Disk Drive LEDs

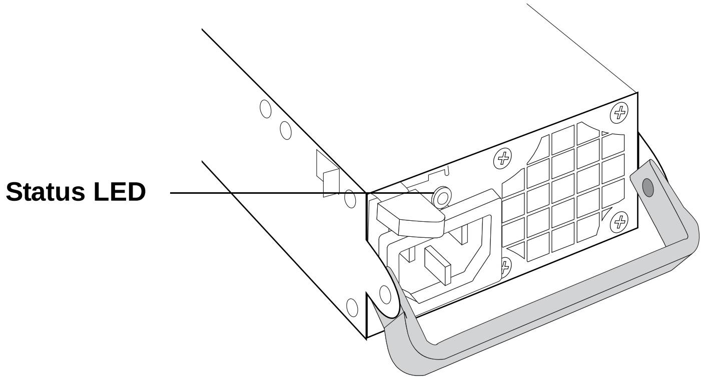
Disk drive LEDs on these SnapServers are located beneath the status lights on the bezel. For all disk drive LEDs, the left light indicates drive status; the right light indicates drive activity. They operate as follows:

Status LED (left)	Activity LED (right)	
Solid green	Off (SATA drive) Solid green (SAS drive)	Disk drive installed properly but is not active
Solid green	Blinking green	Disk drive installed properly and is active

Status LED (left)	Activity LED (right)	
Solid amber	Off	Disk drive installed, but not working correctly
Off	Off	No disk drive installed

Power Supply Module Indicator Lights

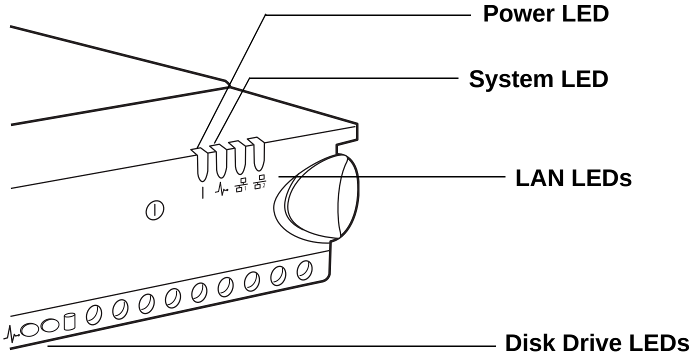
The LED on a 500/600 Series power module is identified in the following illustration.



Power	Description
Solid green	The module is operating properly.
Blinking green	The module has failed or is not connected.
Solid amber **Off**	The module has failed, is not connected, or the server has been turned off.

SnapServer 4200/4500 Status and Drive Light Behavior

The server has two status lights, two network lights, and two lights for each of the four disk drives, as shown in the following illustration:



Overland Storage recommends that you become familiar with the operation of these lights.

Power, System, and LAN LEDs

These status lights are located to the right of the power button. Looking at the server from the front, the lights appear in the following order, from left to right: power LED, system LED, LAN 1 (Ethernet1) LED, and LAN 2 (Ethernet2) LED.

The LEDs operate as described in the following tables:

Power LED	
Solid green	The server is powered on.
Off	The server is powered off.

System LED	
Double-blink green	The server is booting up.
Triple-blink green	The server is shutting down.
Solid or blinking amber at boot time	A problem was detected. The server will not boot.

System LED	
Blinking amber during normal operation	A thermal or other system problem was detected
Blinking amber and green	The server is in Maintenance Mode.

LAN 1 and LAN 2 LEDs	
Solid green	The server is active and connected to the network on the network port.
Off	The port is disconnected or the Ethernet cable is not connected or linked to an active switch.

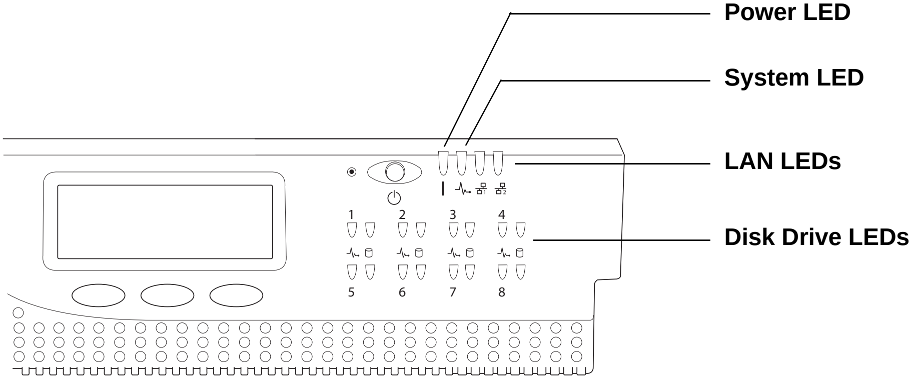
Disk Drive LEDs

Disk drive LEDs on these SnapServers are located at the base of the bezel. The left light indicates drive status. The right light indicates drive activity. They operate as follows:

Status LED (left)	Activity LED (right)	
Solid green	Off	Disk drive installed properly but is not active
Solid green	Blinking green	Disk drive installed properly and is active
Solid amber	Off	Disk drive installed, but not working correctly
Off	Off	No disk drive installed

SnapServer 18000 Status and Drive Light Behavior

The server has two status lights, two network lights, and two lights for each of the eight disk drives, as shown in the following illustration:



Power, System, and LAN LEDs

Looking at the server from the front, the lights appear in the following order, from left to right: power LED, system LED, LAN 1 (Ethernet1) LED, and LAN 2 (Ethernet2) LED. The LEDs operate as described in the following tables:

Power LED	
Solid green	The server is powered on.
Off	The server is powered off.

System LED	
Double-blink green	The server is booting up.
Triple-blink green	The server is shutting down.
Solid or blinking amber at boot time	A problem was detected by BIOS. The server will not boot.
Blinking amber during normal operation	A thermal or other system problem was detected
Blinking amber and green	The server is in Maintenance Mode.

LAN 1 and LAN 2 LEDs	
Solid green	The server is active and connected to the network.
Off	The port is disconnected; or the Ethernet cable is not connected or linked to an active switch.

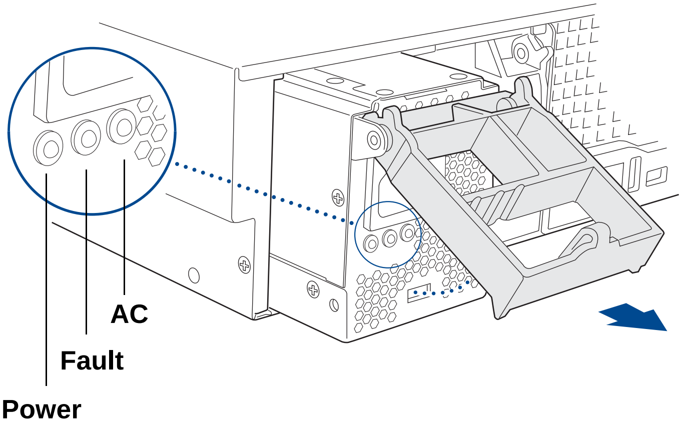
Disk Drive LEDs

Disk drive LEDs on the SnapServer 18000 are located on the bezel to the right of the LED display. The left light indicates drive status. The right light indicates drive activity. The LEDs operate as described in the following table:

Status LED (left)	Activity LED (right)	
Solid green	Off	Disk drive installed properly but is not active
Solid green	Blinking green	Disk drive installed properly and is active
Solid amber	Off	Disk drive installed, but not working correctly
Off	Off	No disk drive installed

Power Supply Module Indicator Lights

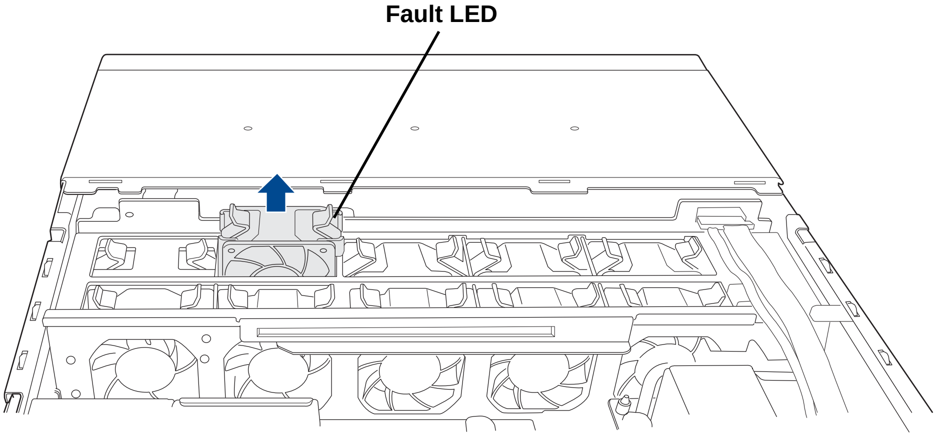
The LEDs on an 18000 power module are identified in the following illustration.



Power	Fault	AC	Description
Solid green	Off	Solid green	The module is operating properly.
Off	Solid red	Solid green	The module has failed.
Off	Off	Off	The module is not connected.

Fan Module LED Indicator Lights

The SnapServer has no external LEDs that indicate the status of a fan module. The **Monitoring > Status** screen of the Administration Tool indicates when a fan has failed. When the cover of the chassis is removed, the Fault LED on the failed module will be lit. The Fault LED of a SnapServer 18000 fan module is identified in the following illustration. To remove a failed fan module, squeeze its handles together and lift the module out of the unit.

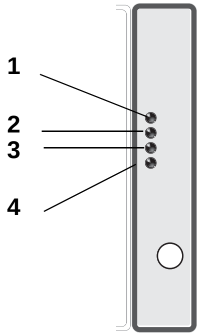


Snap Expansion S50 Enclosure, Disk Drive, APC Module, and Controller Behavior

This section describes the LED indicators on the Snap Expansion S50 enclosure, disk drives, and APC modules.

Enclosure LEDs

On the right front of the Snap Expansion S50 (as shown in the following illustration) are four LEDs that indicate the status of the enclosure.

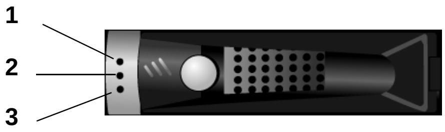


These LEDs operate as described in the following table:

LED	Condition	Indication
1	On	Enclosure power on.
2	On	Fault on enclosure. When a failure occurs on a controller or APC unit, the enclosure LEDs indicate an enclosure fault.
3	Solid green	Host Link. A solid green LED indicates communication with the SnapServer.
4	Rapidly flashing green	Unit ID. Identifies the expansion unit when you click the expansion unit ID link in the Disks and Units screen.

Disk Drive LEDs

Each disk drive has three LEDs that indicate the status of the disk drive.

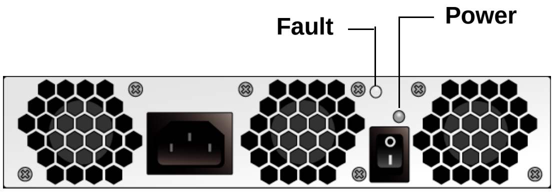


These LEDs operate as described in the following table:

LED	Condition	Indication
1	N/A	Not used.
2	Solid green	Drive present and OK.
	Solid amber	Drive failed.
	Off	Drive not present
3	Solid green	Drive present and idle.
	Green random flash	I/O activity on disk drive.
	Off	Drive not present.

APC Unit LEDs

Each APC unit has two LEDs that indicate status.



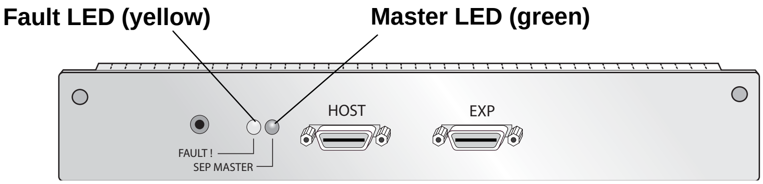
These LEDs operate as described in the following table:

LED	Condition	Indication
Power	Off	Enclosure not powered on.
	Green (solid)	APC unit functioning normally.
Fault	Off	APC unit functioning normally.
	Yellow (flash)	APC unit failure predicted.
	Yellow (solid)	APC unit failed.

When an APC unit fails, the enclosure LED on the front of the unit also indicates the failure.

Controller LEDs

The controller has two LEDs that indicate status.



These LEDs operate as described in the following table:

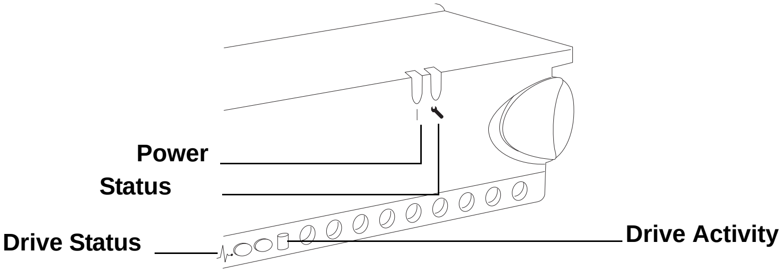
LED	Condition	Indication
Master	On	Controller is current Master for enclosure.
Fault	On 5-10 seconds only	Enclosure is powering on.
	On continuously	Fault condition exists on controller

Snap Disk 10 Disk Drive and Power Supply Module LEDs

This section describes the LED indicators on the Snap Disk 10's disk drives and power module.

Disk Drive LEDs

The Snap Disk 10 has two lights below each disk drive. The Power light (left) indicates power. The Status light (right) indicates system activity.



The LEDs operate as described in the following table:

Drive Status	Drive Activity	Condition of Disk Drive
Green	Amber, flashing	Disk drive installed and being accessed
Green	Not lit	Disk drive installed properly but not being accessed
Amber	Not Lit	Disk drive installed, but not working correctly
Not Lit	Not Lit	No disk drive installed

Power Module LED

The Snap Disk 10 power module has a single LED. The LED operates as described in the following table:

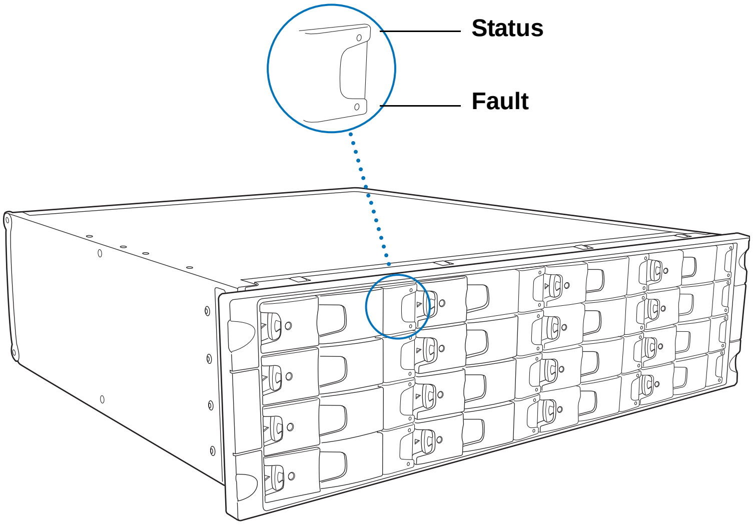
Power Light	Condition of Disk Drive
Solid Green	Power module is installed and working properly
Off	Power module is disconnected, not fully seated, or has failed.

Snap Disk 30SA Disk Drive and Power/Fan Module Behavior

This section describes the LED indicators on the Snap Disk 30SA disk drives and power /fan modules.

Disk Drive LEDs

The Snap Disk 30SA has two LEDs at the edge of each disk drive as shown in the following illustration.

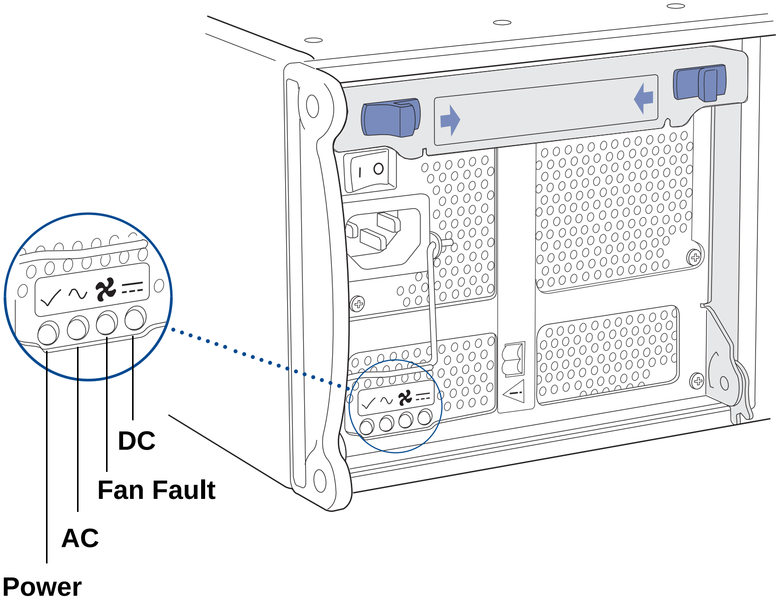


The LEDs operate as described in the following table:

Status	Fault	Condition of Disk Drive
Solid green	Off	Disk drive installed properly but is not active
Solid green	Off	Disk drive installed properly but is not active
Solid green	Solid amber	Disk drive installed, but not working correctly
Off	Off	No disk drive installed

Power and Fan Module LEDs

The Power/Fan module has four LED indicators as shown in the following illustration. To remove the module, squeeze the two latches on the handle together and then withdraw the module by pulling the handle towards you.

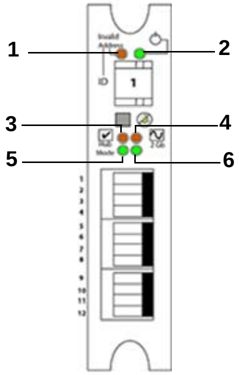


The LEDs operate as described in the following table:

Power	AC	Fan	DC	Condition of Power/Fan Module
Green	Off	Off	Off	Power and fan working properly
Off	Amber	Off	Amber	AC power supply is disconnected
Green	Off	Red	Off	Fan installed, but not working correctly
Off	Off	Off	Off	Module not seated properly or disconnected from operating host server

Ops Panel LEDs

The SD30SA Ops Panel has six LEDs, which are shown in the following illustration.



The LEDs operate as follows:

#	LED	Normal Status	Fault	Description
1	**Invalid Address**	Off	Flashing amber	Invalid Enclosure ID has been selected or the selection has changed since Power On
2	**Power On**	Solid green	Off	Enclosure powered on
3	**System Fault**	Solid amber	Off	System/SCM fault
4	**PSU Fault**	Solid amber	Off	PSU cooling fault or enclosure over- temperature
5	**Hub Mode**	not used	not used	n/a
6	**2GB Link Speed**	not used	not used	n/a

System Reset Options

Often the first thing to try in resolving anomalous behavior on a SnapServer is to reset the server to factory defaults. This section provides information about the following ways to reinstall or reset the system defaults.

- Maintenance Mode
- Resetting the SnapServer to Factory Defaults
- Performing System Resets Without Network Access

Maintenance Mode

You will encounter the SnapServer maintenance mode when the GuardianOS has been compromised and is in need of repair or reinstallation. Maintenance mode consists of a series of HTML screens that allow you to perform the following functions:

- **Upgrade/Repair —** Either upgrades the GuardianOS from one version to another, or applies the GuardianOSImage, but preserves system settings.
- **Fresh install —** Reinstalls the GuardianOS, overwriting any previous configurations and destroying all disk partitions.

Note To install the GuardianOS, you must obtain the appropriate GuardianOSImage file. This file is available from Overland support.

Resetting the SnapServer to Factory Defaults

The GuardianOS allows you to reset different components of the system. Default settings can be found in the default configuration sections of this Guide.

Caution Each reset option requires a reboot of the server. To prevent possible data corruption or loss, make sure all users are disconnected from the SnapServer before proceeding.

Navigate to the **Maintenance > Factory Defaults** screen, select one of the following options, and then click **OK**:

- **Reset Network Configuration To Factory Defaults** Returns TCP/IP and other protocol settings to factory defaults.
- **Reset System Settings, Network, and Admin Passwords To Factory Defaults** Returns the admin and root passwords to the default value, returns TCP/IP and other protocol settings to factory defaults, eliminates all shares to all volumes, and returns settings for server name, date and time, users, groups, quotas, and the activation and configuration of CA *e*Trust Antivirus to factory default values.

When the server finishes rebooting, the Login dialog box opens. Enter the default admin password of `admin`, and click **OK**. The Initial Setup Wizard runs, allowing you to reset the server name, admin password, and IP address.

- **Reset To Default ACLs For Volume** <*`volume name`*> Resets the file and directory security on selected volumes. Volumes and snaptrees are all set to the Windows/ Mixed security model. All files and directories are set to the Windows personality with a Windows ACL that gives full access to Administrators, read access to Everyone, file/directory create access to Everyone (for directories), and full access to the owner (owners are retained in the reset operation).
  - You cannot initiate a reset to defaults if a Snaptree conversion is in progress.
  - Rebooting or shutting down the server in the middle of an ACL reset will halt the operation, and it will not recommence on reboot.

Performing System Resets Without Network Access

Should access to the server be lost, the Reset or LCD panel buttons can be used to reset server settings and re-establish connectivity.

To Perform a Limited Reset Using the Reset Button

On SnapServer 4200 and 4500, the **Reset** button is a white button located to the left of the black power button underneath the front bezel. On the SnapServer N2000, the Reset button is located below the Power button on the server flange. On all other SnapServers, the Reset button is accessed via a small hole next to the Power button on the front of the server. Verify that the server is fully booted (as indicated by the System LED blinking once per second), and push the **Reset** button. The system will reboot after about a minute. As a part of the reset and reboot process, the SnapServer does the following:

- Clears user-defined settings such as DHCP configuration
- Resets the server name to its default setting (`SNAP<server number>`)
- Resets network speed and bonding settings to their defaults
- Resets the Administrator password to the default (`admin`)
- Resets the web server to allow http

Networking Issues

These are some of the networking issues you may encounter when using your SnapServer.

The Server Cannot Be Accessed over the Network

Inaccessibility may be caused by a number of reasons. To resolve this issue, use one of the following methods:

- Verify that you have the correct IP address of the server, and try to connect again.
- Verify that the LED for the primary Ethernet port is lit. (This light indicates network connectivity.) If the light is not lit, perform the following in order:
  - The most likely cause is the physical connection. Check for a loose or damaged cable, or poor connections in the port connector.
  - This problem may also be caused by a mismatch between the settings on the switch or hub and the settings on the SnapServer Ethernet port. These settings must match. To resolve the problem, make sure the port settings on the hub or switch match the settings for the primary port as configured on the **Network > TCP/IP** screen of the Administrator Tool. Use the autonegotiate setting on both the switch and the server port.

You Have No Access to the SnapServer via HTTP

When trying to access the SnapServer via HTTP, the Web browser times out. The server can be accessed using the ping command or Windows Explorer.

- HTTP and HTTPS are both enabled by default on SnapServers. Try typing HTTPS in the Web address rather than HTTP. If you are able to access the server via HTTPS, you can re-enable HTTP on the **Network > Web** screen.
- If you cannot access the server via HTTPS, try resetting the server as described on "Resetting the SnapServer to Factory Defaults" on page 203.

An Access Denied Message Appears after Configuring Microsoft Domain Security

Customers who have configured local users and local groups with the same name as their domain users and groups can have security conflicts if they integrate with Microsoft Domain Security. The SnapServer will authenticate the users as local SnapServer users before authenticating through the Domain. However, the Domain users/groups may be the ones that had been granted access to the shares.

Be careful not to add local users or groups that are duplicates of those that are found on the Windows domain controller.

The SnapServer Does Not Operate Properly on a Network Running Gigabit-Full-Duplex

For Gigabit Ethernet to operate properly, both the switch and the SnapServer's primary Ethernet port must be set to *Auto* (autonegotiate). Any other setting will result in unexpected behavior and reduced performance.

The Network Does Not Have a DHCP Server and the SnapServer IP Address Is Unknown

Install SnapServer Manager from the SnapServer User CD onto a client workstation on the same subnet as the SnapServer. You can then use the utility to discover all SnapServers on that network segment, and to assign static IP addresses as necessary.

Apple Users Cannot Log into the SnapServer as Windows Users

To allow Apple users to access a SnapServer, replicate their user names and passwords locally on the SnapServer.

An Apple Mac Connection to the SnapServer Is Reset When a Share Is Updated

A Mac client connected to a SnapServer share may receive a message stating that the SnapServer will be going down in 5 minutes. This is because the AFP protocol needs to be restarted. To resolve this issue, reconnect to the share.

Problems Occur with Domain Controller Authentication

You are receiving the following errors in your error log:

```
SMB: Domain Controller unavailable
SMB: Username not connected to Domain Controller
```

This means that either your Domain Controller is down, or the SnapServer is unable to reach it. Because it cannot communicate with the Domain Controller, it is not able to authenticate the user. Check to make sure the Domain Controller is online, is consistently reachable via the network, and that users can authenticate to the Domain Controller.

You Start Your SnapServer but Cannot See It on the Network

10.10.10.10 is the default address for the primary Ethernet port if no DHCP server is seen on your network. Ensure that the Ethernet cable is connected securely to both the network port and the server's primary Ethernet port. Also, check to see that the Link light on the front of the SnapServer is lit (solid green). If the Link light is off, this is normally caused by a mismatch between the switch/hub and the Ethernet port on the SnapServer. To resolve this problem, verify that all settings (if using multiple Ethernet ports) on the switch/hub match the setting on the server. When the server is shipped from the factory, both ports are set to autonegotiate. Therefore, the switch/hub *must* be set to autonegotiate to initially connect to the server.

The NT Event Viewer Reports Forced Master Browser Election When SnapServers Are Online

SnapServers have the ability to act as a master browser on a Microsoft network. This may cause a message to appear in an NT server's event log about a forced master browser election.

SnapServers should lose elections to Windows domain controllers (NT/2K/2K3), but win against standalone Windows servers (NT/2K/2K3) and workstations (all versions); however, users often prefer to prevent this election entirely.

The master browser option is enabled by default on SnapServers to allow them to appear more rapidly in a peer-to-peer Windows environment. In some environments that include NT server systems, this may cause the NT server to show warnings about having to force a master browser election in the event log. You can prevent these warning messages by disabling the Master Browser option on the **Network > Windows** screen.

You Try to Mount to a Share on Your SnapServer from Your Linux Workstation and You Receive an RPC Timeout Message

Check the firewall configuration to your Linux workstation. Be sure you have not blocked the ability to receive TCP or User Datagram Protocol (UDP) communications. If problems persist, contact Overland Storage Technical Support.

You Receive an Access Denied Message When Attempting to Mount a Share on Your SnapServer from a Linux Workstation

If you are logged in as *root* on your workstation and NFS is enabled on your SnapServer, this message can be misleading, causing you to look for security issues, when in fact it could be a command syntax issue. For example, the common Linux mount command:

```
mount 192.168.32.124:SHARE1 /mnt
```

is missing a forward slash (/) in the command, which will return an Access Denied message. The correct syntax should be the following:

```
mount 192.168.32.124:/SHARE1 /mnt
```

Note The share name is case sensitive.

You Cannot Log in as Root to the SnapServer

GuardianOS allows you to log in as root over SMB. If this operation has failed or you have trouble logging in, be sure that you have enabled root login in the **Network > Windows** page. Also note that the root account password is tied to the admin account password. If you cannot log in as root, change the password for the admin account on the **Network > Windows** screen. Use the admin password to log in as root.

Snap Disk 10 Disk Drives do not Appear on the Storage > Disks/Units Screen

Verify that the Snap Disk 10 is connected properly to the Serial ATA connector at the rear of the SnapServer and that the expansion array is properly connected to the power supply. Then, to initialize the Snap Disk 10, power off and then power on the SnapServer.

Caution Make sure to use a screwdriver to firmly seat the connectors on the Snap Disk 10 and the SnapServer. Tightening the connectors by hand will not work.

You Are Unable to See Your Domain Users When Trying to Set Up Windows Security Permissions on File Folders

The SnapServer (GuardianOS) has joined the Active Directory domain properly, and you can see the domain users when you set Share permissions from the browser-based Administration Tool.

Make sure the Windows client (PC) you are trying to set permissions from is assigned a valid DNS server. You can check your Windows client using the `ipconfig` command from a command prompt.

Miscellaneous Issues

These are some miscellaneous issues you may encounter when using your SnapServer.

Back Up Applications

You Backed Up Your Snapshot Share, Are Now Attempting to Restore It, and the Operation Fails

A snapshot share is read-only. You can restore the data to a read-write accessible share.

The NetVault Client Cannot Connect to the NetVault Server on the SnapServer

Occasionally, after enabling NetVault for GuardianOS for the first time, the NetVault for GuardianOS Server may not start properly. If this happens, the

NetVault client application may not be able to connect to the NetVault for GuardianOS server running on the SnapServer. To resolve this issue, simply disable and then re-enable the NetVault for GuardianOS Server via the **SnapExtensions > BakBone NetVault** screen.

BakBone NetVault Restore Limitations for UNIX SnapTrees

File and directory permissions will be restored when using BakBone NetVault. However, when Windows file and directory permissions are restored to a UNIX SnapTree on a SnapServer, the Windows-style extended permissions are removed to preserve proper UNIX Snaptree permissions.

When Backing Up with Symantec Backup Exec 9.1 or 10.0, the Backup Hangs

To resolve this issue immediately, restart the Backup Exec server.

Other Issues

A Problem Occurred While Booting. The System is Offline and the Status LED is Blinking Amber and Green

The SnapServer has booted into Maintenance (Recovery) Mode. This may be due to a boot failure in the previous boot attempt. Try booting again. If the server still returns to Maintenance Mode, call Technical Support.

Power to the SnapServer Is Unexpectedly Cut Off Due to a Power Outage

Overland Storage recommends that you use an uninterruptible power supply (UPS) with the SnapServer. If you did not have a UPS attached to the server at the time of the power outage, do the following:

1. On SnapServers with no on/off switch, remove the power cables. On Snap Expansion S50 and SD30SA, turn off the power switches on the back of the unit.
2. Once the power is restored and stabilized, turn the power supplies back on and reboot the server.

   Once the SnapServer boots, it begins resynchronizing the RAID(s) if necessary. You can use the server during the resynchronization, but performance will be a little slower than normal. Do not remove drives, however, while the server is resynchronizing the RAID.

The Server Is Not Responding to File Requests or Configuration Commands

Call your SnapServer technical support representative.

Problems with Cable Arm on the 18000 with a SCSI Cable Attached

The size of the connector on an attached SCSI cable may prevent the 18000 from fully withdrawing into a rack when the cable management arm is attached. To resolve this problem, remove the cable management arm.

You Have Problems Seeing the Tape Library Tape Device, Not the Robotic Arm

When you have problems seeing the actual tape device rather than the robotic arm, it is most likely due to the Tape Loader being configured for Sequential Access. Change the Tape Loader to Random or Mixed Mode.

The Admin Password to the Administration Tool Is Not Available

You can perform a limited reset to defaults, which includes the admin password (as described in “Performing System Resets Without Network Access” on page 204); then use the Administration Tool to set a new password.

The SnapServer 510, 520, 550, 620, 650, or 18000 LCD is Flashing

A flashing LCD indicates a server panic. In some cases, rebooting the server may solve the problem. However, if this condition occurs more than once, try resetting the system as described in “Performing System Resets Without Network Access” on page 204.

You Can Not Delete Files or Folders From an iSCSI Disk

If an iSCSI disk is mounted to a folder, not a letter drive, in Windows you will not be able to delete files and folders inside that mount point. The Windows Recycle Bin does not understand mount points, so to avoid this problem either mount iSCSI disks to letter drives on your Windows OS, or hold down the shift key while deleting folders or files.

Phone Home Support

Once your SnapServer has been registered, Phone Home Support becomes available for use. Phone Home Support emails system logs and files that contain information useful for troubleshooting purposes to Overland Storage technical support. You can use the **Monitor > Support** screen to open a new case with technical support; or, in the course of working to resolve an issue, a technical support representative may ask you to fill out and submit this page. If a case is already in progress, you will need to enter the case number provided by the technical support representative.

Notes Phone Home Support interacts with two fields on the **Server > Email Notification** screen: (1) To use Phone Home Support, you must enter a valid SMTP server IP address on the Email Notification screen; and (2) the first email address listed in the Recipient(s) field populates the Admin Email Address field on the Support screen.

Complete the following fields as appropriate, then click **OK**:

Text Field	Description
Subject	(Required) Enter a concise description that identifies the issue.
Case	(Required) Select *New Case* if you are emailing technical support for the first time. Select *Existing Case* if you have previously contacted technical support concerning the issue.
Case Number	If you selected *Existing Case* above, enter the case number provided by technical support.
Reply-to Address	(Required) This field defaults to the first email address entered as a recipient on the **Server > Email Notification** screen. If necessary, enter at least one email address that will serve as the contact email address for this issue. To receive a copy of the email and system information attachment, select the *Cc Admin* check box.
Comments	(Required) Enter additional information that will assist in the resolution of the problem.

GuardianOS Ports

The following table outlines the ports used in the GuardianOS.

Port #	Layer	GOS Feature	Name	Comment
1	DDP		rtmp	Routing Table Management Protocol
1	TCP & UDP		tcpmux	TCP port service multiplexer
2	DDP		nbp	Name Binding Protocol
4	DDP	Network > Apple	echo	AppleTalk Echo Protocol
6	DDP	Network > Apple	zip	Zone Information Protocol
21	TCP & UDP	Network > FTP	ftp	File Transfer Protocol (FTP) port; sometimes used by File Service Protocol (FSP)
22	TCP & UDP	Server > SSH	ssh	Secure Shell (SSH) service
25	TCP & UDP	Server > Email Notification	smtp	Simple Mail Transfer Protocol (SMTP)
67	TCP & UDP	Network > TCP/IP	bootps	Bootstrap Protocol (BOOTP) services; also used by Dynamic Host Configuration Protocol (DHCP) services
68	TCP & UDP	Network > TCP/IP	bootpc	Bootstrap (BOOTP) client; also used by Dynamic Host Control Protocol (DHCP) clients
80	TCP & UDP	WebUI	http	HyperText Transfer Protocol (HTTP) for World Wide Web (WWW) services

Port #	Layer	GOS Feature	Name	Comment
81	TCP	WebUI	HTTP	Hypertext Transport Protocol
88	TCP & UDP	Network > NFS	Kerberos	Kerberos Security (NFS v4)
111	TCP & UDP	• Networking > NFS • Assist • SnapServer Manager	sunrpc	Remote Procedure Call (RPC) Protocol for remote command execution, used by Network Filesystem (NFS) and SnapServer Manager
123	TCP & UDP	Server > Date/Time > Advanced	ntp	Network Time Protocol (NTP)
137	TCP & UDP	Network > Windows	netbios-ns	NETBIOS Name Services used in Red Hat Enterprise Linux by Samba
138	TCP & UDP	Network > Windows	netbios-dgm	NETBIOS Datagram Services used in Red Hat Enterprise Linux by Samba
139	TCP & UDP	Network > Windows	netbios-ssn	NETBIOS Session Services used in Red Hat Enterprise Linux by Samba
161	TCP & UDP	Network > SNMP	snmp	Simple Network Management Protocol (SNMP)
162	TCP & UDP	Network > SNMP	snmptrap	Traps for SNMP
201	TCP & UDP	Network > Apple	at-rtmp	AppleTalk routing
202	TCP & UDP	Network > Apple	at-nbp	AppleTalk name binding
204	TCP & UDP	Network > Apple	at-echo	AppleTalk echo
206	TCP & UDP	Network > Apple	at-zis	AppleTalk zone information
389	TCP & UDP	Network > Windows	ldap	Lightweight Directory Access Protocol (LDAP)

Port #	Layer	GOS Feature	Name	Comment
443	TCP & UDP	• WebUI • SnapServer Manager • SnapExtension > Snap EDR	https	Secure Hypertext Transfer Protocol (HTTP).
445	TCP & UDP	Network > Windows	microsoft-ds	Server Message Block (SMB) over TCP/IP
515	TCP	Server > Printing		LPD (Linux Printer Daemon)/LPR (Linux Printer Remote
548	TCP & UDP	Network > Apple	afpovertcp	Appletalk Filing Protocol (AFP) over Transmission Control Protocol (TCP)
631	TCP & UDP	Server > Printing		IPP (Internet Printing Protocol)/CUPS (Common UNIX Printing System)
852	TCP	Network > NFS		Used by rpc.mountd
882	UDP	• Snap Finder • SnapServer Manager	Sysbroker	Broadcast Discovery
933	UDP	Network > NFS		Used by rpc.statd
936	UDP	Network > NFS		Used by rpc.statd
939	TCP	Network > NFS		Used by rpc.statd
957	UDP	Assist		Used by assistrecv
959	TCP	Assist		Used by assistrecv
2005	TCP	SnapExtensions	SnapExtensions	Bridge from Servlet to Snap Extension framework
2049	TCP & UDP	Network > NFS	nfs [nfsd]	Network File System (NFS)
2050	UDP	Network > NFS	mountd	
2599	UDP	• Snap Finder • SnapServer Manager	Sysbroker	Multicast Discovery
3052	TCP	Server > UPS		Port for monitoring UPS status

Port #	Layer	GOS Feature	Name	Comment
3205	TCP	Network > iSCSI	iSNS	
3260	TCP	Network > iSCSI	iSCSI	
8001	TCP	SnapExtension > SnapEDR	SnapEDR	External Communications
8002	TCP	SnapExtension > SnapEDR	SnapEDR	External Communications
8003	TCP	SnapExtension > SnapEDR	SnapEDR	External Communications
8005	TCP	WebUI	tomcat	Tomcat Shutdown port
8008	TCP & UDP	Web UI	http-alt	Tomcat - Apache Bridge
9049	TCP	Sysbroker		Sysbroker Shutdown Port
9050	TCP	Sysbroker		Sysbroker RPC Port
10000	TCP	SnapExtension > BakBone NetVault	NetVault	
10001	TCP	Snap Extension	Snap Extension	Shutdown Port
12000	TCP & UDP	Network > Apple	afp2overtcp	Second NIC
12168	TCP	CA Antivirus	inoweb	Admin Interface
16384	UDP		Sysbroker	Random Port
16388	UDP		Sysbroker	Random Port
20031	TCP	SnapExtension > BakBone NetVault	NetVault	Listening Port
24066	TCP		poolmgr	Used by /bin/poolmgr
32780	TCP	WebUI	tomcat	Random Port
32781	TCP	WebUI	tomcat	Random Port
49221	TCP	SnapExtension > SnapEDR	SnapEDR	External Communications Port
49229	TCP	SnapExtension > SnapEDR	SnapEDR	External Communications Port
1024 - 65535	TCP & UDP	• Network > NFS • Network > FTP	NFS FTP (passive)	Dynamically allocated in runtime for user connections

Term	Definition
access permissions	A rule associated with a share, a file, or a directory to regulate which users can have access to the share and in what manner.
ACL (Access Control List)	The list that controls access to directories and files. Each ACL includes a set of access control entries, which contain the metadata that the system uses to determine access parameters for specified users and groups.
Administration Tool	A Web-based utility used for configuration and ongoing maintenance, such as monitoring server conditions, configuring email alerts for key events, or for SNMP management.
ADS (Active Directory Service)	The preferred authentication method for Windows XP, Windows 2000, Windows 2000 Advanced Server, and Windows 3000 network users. This authentication allows Active Directory users to connect to shares on the SnapServer. The SnapServer supports the Microsoft Windows 2000 family of servers that run in native ADS mode or in mixed NT/ADS mode.
AFP (AppleTalk Filing Protocol)	A Local Area Network (LAN) architecture built into all Apple Macintosh computers.
agent	A program that performs some information-gathering or processing task in the background. SnapServers support Data Protection Agents and can be configured as SNMP agents.
algorithm	A sequence of steps designed to solve a problem or execute a process.
AllLocalUsers group	The default group for all local users on SnapServers. Local users are set up by the SnapServer administrator. Network users or Windows domain users are not part of the AllLocalUsers group.
AllUsers group	A collection of all users. The SnapServer automatically maintains the AllUsers group.
array	A series of objects, all of which are the same size and type. In a server context, an array refers to the grouping of hard drives into a RAID set.

Term	Definition
authentication	The validation of a user’s identity by requiring the user to provide a registered login name and corresponding password.
autonegotiation	An Ethernet feature that automatically negotiates the fastest Ethernet speed and duplex setting between a port and a hub or switch. This is the default setting and is recommended.
autosensing	An Ethernet feature that automatically senses the current Ethernet speed setting.
bonding	A technology that treats two ports as a single channel, with the network using one IP address for the server. SnapServers support load balancing and failover bonding modes.
CA *e*Trust Antivirus	The antivirus software bundled with the SnapServer.
chaining	A native SnapServer technology in which all snapshots of a volume depend on successive snapshots for part of their content.
channel	A communications path between two computers or devices.
CHAP (Challenge Handshake Authentication Protocol)	CHAP verifies the identity of the peer using a three-way handshake.
checksum	The result of adding a group of data items that are used for checking the group. The data items can be either numerals or other character strings treated as numerals during the checksum calculation. The checksum value verifies that communication between two devices is successful.
CIFS (Common Internet File System)	The default Windows protocol for communication between computers. A specification for an Internet file access protocol that complements HTTP and FTP and reduces access time.
daemon	A process that runs in the background.
default gateway	The router used when there is otherwise no known route to a given subnet.
degraded	A RAID state caused by the failure or removal of a disk drive in which data is consistent, but there is no redundancy.
DHCP (Dynamic Host Configuration Protocol)	A communications protocol that lets network administrators centrally manage and automate the assignment of IP addresses on a computer network. Each system that connects to the Internet/intranet needs a unique IP address. The SnapServer can be configured to perform as a DHCP server and assign IP addresses with a single subnet.

Term	Definition
directory	A virtual folder used to organize files. Also called a folder.
disaster recovery	A strategy that allows a company to return to normal activities after a catastrophic interruption. Through failover to a parallel system or by restoration of the failed system, disaster recovery restores the system to its normal operating mode.
disk	A rigid platter, usually constructed of aluminum or mylar, with a magnetic surface that allows the recording of data, that is stored inside the drive.
DNS server (Domain Name System server)	The server that maintains a mapping of all host names and IP addresses. Normally, this mapping is maintained by the system administrator, but some servers support dynamic mappings.
domain	A set of network resources in Windows NT and Windows 2000/2003/2008, such as users and groups of users. A domain may also include multiple servers on the network. To gain access to these network resources, the user logs into the domain.
domain name	The ASCII name that identifies the domain for a group of computers within a network.
Ethernet	The most widely installed LAN technology. 100Base-T Ethernet provides transmission speeds of up to 100 Mbps. Fast Ethernet or 1000Base-T provides transmission speeds up to 1000 Mbps and is typically used for LAN backbone systems, supporting workstations with 100Base-T cards. Gigabit Ethernet (GbE) provides an even higher level of backbone support at 1000 Mbps (one Gigabit or one billion bits per second).
Ethernet address	The unique six-digit hexadecimal (0-9, A-F) number that identifies the Ethernet interface.
Ethernet port	The port that houses the network card to provide Ethernet access to the computer.
event	Any significant occurrence in the system that may require notifying a system administrator or adding an entry to a log.

Term	Definition
failover	A strategy that enables one Ethernet port to assume the role of another port if the first port fails. If a port fails on a SnapServer, the second port assumes its network identity (if the two Ethernet cards have been configured for failover). When the port comes back online, the original identities are restored. Failover is possible only in a multi-Ethernet configuration.
FTP (File Transfer Protocol)	A standard Internet protocol that provides a way to exchange files between computers on the Internet. By default, a SnapServer is set up to be an FTP server.
full-duplex	A type of transmission that allows communicating systems to both transmit and receive data simultaneously.
gateway	The hardware or software that bridges the gap between two network subnets. It allows data to be transferred among computers that are on different subnets.
GID (group IDs)	On a SnapServer, the unique ID assigned to each group for security purposes.
GuardianOSImage.gsu	An image file used to upgrade the GuardianOS.
half-duplex	A type of transmission that transfers data in one way at a time.
hidden share	A share that restricts the display of the share via the Windows (SMB), Web View (HTTP/HTTPS), FTP, and AFP protocols.
host name	The unique name by which a computer is known on a network. It is used to identify the computer in electronic information interchange.
hot spare (local or global)	A disk drive that can automatically replace a damaged drive in a RAID 1 or 5. If one disk drive in a RAID fails or is not operating properly, the RAID automatically uses the hot spare to rebuild itself without administrator intervention. A *local* hot spare is associated with and available only to a single RAID. A *global* hot spare is associated with a single RAID, but may be used for any RAID in the system.
hot swapping	The ability to remove and add disk drives to a system without the need to power down or interrupt client access to file systems.
HTTP (Hypertext Transfer Protocol)	An application protocol for transferring files (text, graphic images, sound, video, and other multimedia files) over TCP/IP on the World Wide Web.

Term	Definition
HTTPS (Hypertext Transfer Protocol Secure)	The HTTP protocol using a Secure Sockets Layer (SSL). SSL provides data encryption, server authentication, message integrity, and client authentication for any TCP/IP connection.
I/O (Input/Output)	The operation of transferring data to or from a device, typically through an interface protocol like CIFS, NFS, or HTTP. The SnapServer presents a file system to the user and handles block I/O internally to a RAID array.
Inheritance	In Windows permissions, inheritance is the concept that when permissions for a folder are defined, any subfolders within the defined folder inherit its permissions. This means an administrator need not assign permissions for subfolders as long as identical permissions are desired. Inheritance greatly reduces administrative overhead and also results in greater consistency in access permission management.
IP (Internet Protocol) address	The unique 32-bit value that identifies the location of the server. This address consists of a network address, optional subnetwork address, and host address. It displays as four addresses ranging from 1 to 255 separated by periods.
iSCSI (Internet SCSI)	iSCSI is a standard that defines the encapsulation of SCSI packets in TCP and then routing it using IP. It allows block-level storage data to be transported over widely used IP networks.
Jukebox	A robotic tape backup device that stores numerous tape drives and uses a mechanical arm to bring the drive to a station for reading and writing.
JVM (Java Virtual Machine)	Software that converts Java bytecode into machine language and executes it. A JVM allows an application such as SnapServer Manager written in Java to run on any operating system.
Kerberos	A secure method for authenticating a request for a service used by ADS. Kerberos lets a user request an encrypted “ticket” from an authentication process that can then be used to request a service from a server. The user credentials are always encrypted before they are transmitted over the network. In Windows 2000/XP, the domain controller is the Kerberos server. The Kerberos key distribution center (KDC) and the origin of group policies are applied to the domain.
LCD (Liquid Crystal Display)	An electronic device that uses liquid crystal to display messages on some SnapServers.

Term	Definition
LED (Light-Emitting Diode)	An electronic device that lights up when electricity is passed through it.
Linux	A UNIX-like operating system that was designed to provide personal computer users a free or very low-cost operating system comparable to traditional and usually more expensive UNIX systems. The GuardianOS is based on the Linux operating system.
load balancing	A process available only in multi-Ethernet configurations. The Ethernet port transmission load is distributed among two or more network ports (assuming the cards are configured for load balancing). An intelligent software adaptive agent repeatedly analyzes the traffic flow from the server and distributes the packets based on destination addresses.
local group/local user	A group/user defined locally on a SnapServer using the Administration Tool. The local user is defined by the server administrator. Windows domain, ADS, and NIS users are not considered local.
MAC (Media Access Control)	In the Open Systems Interconnection (OSI) model, one of two sublayers of the Data Link Control layer. Concerned with sharing the physical connection to the network among several computers. Each Ethernet port has a unique MAC address. SnapServers with dual-Ethernet ports can respond to a request with either port and have two unique MAC addresses.
maintenance mode	A series of HTML screens that allow you to perform repair, upgrade, or reinstall the GuardianOS in a disaster recovery situation.
MIB (Management Information Base)	A formal description of a set of network objects that can be managed using the Simple Network Management Protocol (SNMP). The format of the MIB is defined as part of SNMP.
mirroring	Used in RAID 1, a process of storing data on one disk and copying it to one or more disks, creating a redundant storage solution. RAID 1 is the most secure method of storing mission-critical data.
mounted	A file system that is available.
multihomed	A SnapServer that is connected to two or more networks or has two or more network addresses.

Term	Definition
NAS (Network Attached Storage)	Hard disk storage that is set up with its own network address as opposed to being attached to the department computer that is serving applications to a network's workstation users. By removing storage access and its management from the department server, both application programming and files can be served faster because they are not competing for the same processor resources. The NAS device is attached to a local area network (typically an Ethernet network) and assigned an IP address.
NetVault for GuardianOS	A comprehensive backup solution that is preinstalled on SnapServers running GuardianOS 2.6 or higher to support backup and restore operations to a local tape drive.
NFS (Network File System)	A client/server application that allows a computer user to view and optionally store and update files on a remote computer as though they were on the user's own computer. The user's system needs to have an NFS client and the other computer needs the NFS server. The SnapServer is configured as an NFS server by default.
NIS (Network Information Service)	A network naming and administration system for smaller networks that was developed by Sun Microsystems. NIS+ is a later version that provides additional security and other facilities. The SnapServer accepts NIS users and groups.
node	Any device, including servers, workstations, or tape devices, that are connected to a network; also the point where devices are connected.
NVDB (NetVault Database) directory	A NetVault for GuardianOS database directory stored on the SnapServer that holds records for the media and backups performed.
orphan	A disk drive that has become disconnected from its RAID either by accidental removal of the drive or the intermittent failure of the drive.
parity	Error correction data. RAID 5 stores equal portions of each file on each disk and distributes parity information for each file across all disks in the group. This distributed parity allows the system to recover from a single disk drive failure.
Permissions	A security category, such as no access, read-only, or read-write, that determines what operations a user or group can perform on folders or files.
PoP (Proof of Purchase)	The number used to obtain a license key for an upgrade to third-party applications.

Term	Definition
POSIX (Portable Operating System Interface)	A set of standard operating system interfaces based on the UNIX operating system. The need for standardization arose because enterprises using computers wanted to develop programs that could run on multiple platforms without the need to recode. Pre-GuardianOS 5.0 SnapServers use Extended POSIX ACLs.
protocol	A standardized set of rules that specifies the format, timing, sequencing, and/or error checking for data transmissions.
public access share	A share that allows all users read/write access to the file system.
quota	A limit on the amount of storage space on a volume that a specific user or NIS group can consume.
RAID (Redundant Array of Independent Disks)	A collection of disk drives that act together as a single storage system. Different RAID types provide different levels of data protection.
RAID 0 (Striped)	Distributes data evenly among all disks in the array. This technique, called data striping, results in fast access speeds because it uses multiple physical devices to store the data. However, RAID 0 offers no redundancy and does not accept hot spares. If a single disk drive fails, every file in the RAID is rendered unavailable.
RAID 1 (Mirrored)	Stores data on one disk drive and copies it to another drive in the RAID. A RAID 1 must contain at least two disk drives: one for the data space and one for redundancy. Although the data space in a RAID 1 can never be larger than a single drive, some administrators prefer to add a third drive (either as a hot spare or a member) for additional redundancy. RAID 1 is the most secure method for storing mission-critical data because there is no catastrophic data loss when a disk fails. However, RAID 1 is the most expensive and least efficient storage method.
RAID 5 (Striping with Parity)	Distributes data evenly among all disks in the array, and maintains parity information (error correction data) that allows the system to recover from a single disk drive failure. RAID 5 provides the best combination of performance, usability, capacity, and data protection.
RAID 6 (Striping with Dual Parity)	Similar to RAID 5 except that two drives maintain parity information for greater redundancy. System can recover from two drive failures. Provides high reliability and data protection but write performance speed is impacted by the dual parity drives.

Term	Definition
RAID 10 (Striped Mirroring)	RAID 10 is two or more RAID 1's striped together to provide greater redundancy and higher performance than a simple RAID 1.
recurring snapshot	A snapshot that runs at an administrator-specified time and interval.
restrict anonymous	A Windows feature in which anonymous users cannot list domain user names and enumerate share names. Microsoft has provided a mechanism in the Registry called restrict anonymous for administrators to restrict the ability for anonymous logon users (also known as NULL session connections) to list account names and enumerate share names. The implementation of the restrict anonymous mechanism may prevent the SnapServer from obtaining the list of account names it needs to authenticate Windows domain users.
resynchronization	A RAID state that describes the process of integrating a new drive into the RAID.
rollback	A snapshot feature that allows the administrator to restore a volume to a previous state as archived in a snapshot without resorting to tape.
SCSI (Small Computer System Interface)	A parallel interface standard used to attach peripheral devices, such as robotic libraries, to computers.
serial number	The ten-character alphanumeric number assigned by the manufacturer at the factory.
server number	A numeric derived from the MAC address of your SnapServer's primary Ethernet port that is used to uniquely identify a SnapServer.
share	A virtual folder that maps to the root of a volume or a directory on the volume. Permissions are assigned to a share that determine access for specific users and groups.
share access	Permissions granted or denied to users and groups that control user and group access to the files.
SMB (Server Message Block)	A protocol for Windows clients. SMB uses the TCP/IP protocol. It is viewed as a complement to the existing Internet application protocols such as FTP and HTTP. With SMB, you can access local server files, obtain read-write privileges to local server files, share files with other clients, and restore connections automatically if the network fails.

Term	Definition
Snap EDR	A SnapExtension that copies the contents of a share from one SnapServer to another share on one or more SnapServers. Snap EDR is designed to work with SnapServers and other SnapServer Storage Solutions.
SnapServer Manager (SSM)	A Java-based utility for discovering and monitoring SnapServers.
SnapDRImage	The SnapServer disaster recovery image that saves server-specific settings such as server name, network, RAID, volume and share configuration, local user and group lists, and snapshot schedules.
SnapExtension	A Java application that extends a SnapServer's functionality. SnapExtensions are produced both by SnapServer and third-party vendors.
snapshot	A consistent, stable, point-in-time image of a volume (file system) used for backup purposes.
snapshot pool	Disk space reserved within a RAID for the storage of snapshot data. In the default storage configuration of many SnapServers, twenty percent of the RAID capacity is allocated to the snapshot pool.
snapshot share	A virtual folder that allows access to all current snapshots at the same directory level as the original share on which it is based.
SnapTree Directory	A directory residing in the root of a volume that is assigned a Windows- or UNIX-style security model. The security model determines the file-level security scheme that will apply to files, folders, and subdirectories within the SnapTree directory.
SNMP (Simple Network Management Protocol)	A system to monitor and manage network devices such as computers, routers, bridges, and hubs. SNMP views a network as a collection of cooperating, communicating devices, consisting of managers and agents.
SSH (secure shell)	A service that provides a remote console for special system administration and customer support access to the server. SSH is similar to telnet but more secure, providing strong encryption so that no passwords cross the network in clear text.
SSL (Secure Sockets Layer)	A technology that provides data encryption, server authentication, message integrity, and client authentication for any TCP/IP connection.

Term	Definition
standalone	A network bonding mode which treats each port as a separate interface. This configuration should be used only in multihomed environments in which network storage resources must reside on two separate subnets.
static IP address	An IP address defined by the system administrator rather than by an automated system, such as DHCP. The SnapServer allows administrators to use DHCP-assigned or statically assigned IP addresses.
striping	A RAID storage technique that distributes data evenly among all disks in the array.
subnet mask	A portion of a network that shares a common address component. On TCP/IP networks, subnets are all devices with IP addresses that have the same prefix.
TCP/IP (Transmission Control Protocol/Internet Protocol)	A commonly used networking protocol that supports the interconnection of different network operating systems.
trap	A signal from the SnapServer informing an SNMP management program that an event has occurred.
U	A standard unit of measure for designating the height in computer enclosures and rack cabinets. One U equals 1.75 inches. For example, a 3U server chassis is 5.25 inches high.
UI (User Interface)	The User Interface is the graphical and textual presentation of the GuardianOS in your web browser.
UID (User IDs)	A unique ID assigned to each user on a SnapServer for security purposes.
unassigned	The state of a disk drive that is seated in a bay but has not been incorporated into a RAID.
UNC (Universal Naming Convention)	In a network, a way to identify a shared file in a computer without having to specify (or know) the storage device it is on. In the Windows OS, the UNC name format is as follows: \\server_name\share_name\path\file_name
UPS (Uninterruptable Power Supply)	A device that allows a computer to keep running for a short time when the primary power source is lost. It also provides protection from power surges. A UPS device contains a battery that starts when the device senses a loss of power from the primary source.
URL (Uniform Resource Locator)	A Web address.

Term	Definition
Virtual Disk Service (VDS)	Microsoft VDS is a service that extends existing storage capabilities of Windows Server operating systems.
volume	A logical partition of a RAID's storage space that contains a file system. In the default storage configuration of many SnapServers, eighty percent of the RAID capacity is allocated to the default volume.
Volume Shadow Copy Service (VSS)	Microsoft VSS provides a mechanism for creating consistent point-in-time copies of data known as shadow copies.
Web View	The Web-browser screen that opens when users access a SnapServer using their Web browsers, and displays a list of all shares.
Windows domain authentication	Windows-based networks use a domain controller to store user credentials. The domain controller can validate all authentication requests on behalf of other systems in the domain. The domain controller can also generate encrypted challenges to test the validity of user credentials. Other systems use encrypted challenges to respond to CIFS/SMB clients that request access to a share.
WINS (Windows Internet Naming Service)	The server that locates network resources in a TCP/IP-based Windows network by automatically configuring and maintaining the name and IP address mapping tables.
workgroup	A collection of computers that are grouped for sharing resources such as data and peripherals over a LAN. Each workgroup is identified by a unique name.